IRPP choices

Vol. 15, no. 9, September 2009 ISSN 0711-0677 www.irpp.org

Accountability in and for National Security

Reg Whitaker and
Stuart Farson

Security and Democracy

IRPP

Founded in 1972, the Institute for Research on Public Policy is an independent, national, nonprofit organization.

IRPP seeks to improve public policy in Canada by generating research, providing insight and sparking debate that will contribute to the public policy decision-making process and strengthen the quality of the public policy decisions made by Canadian governments, citizens, institutions and organizations.

IRPP's independence is assured by an endowment fund established in the early 1970s.

Fondé en 1972, l'Institut de recherche en politiques publiques est un organisme canadien, indépendant et sans but lucratif.

L'IRPP cherche à améliorer les politiques publiques canadiennes en encourageant la recherche, en mettant de l'avant de nouvelles perspectives et en suscitant des débats qui contribueront au processus décisionnel en matière de politiques publiques et qui rehausseront la qualité des décisions que prennent les gouvernements, les citoyens, les institutions et les organismes canadiens.

L'indépendance de l'IRPP est assurée par un fonds de dotation établi au début des années 1970.

Reg Whitaker is distinguished research professor emeritus at York University and adjunct professor of political science at the University of Victoria. He writes on Canadian politics and on security and intelligence, and his publications include *Canada and the Cold War* (2003) and *The End of Privacy: How Total Surveillance Is Becoming a Reality* (1999). He served as a member of the advisory panel to Justice Dennis O'Connor for the second part of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. He also chaired a federal advisory panel to review aviation security. In 2007, this panel also reported on aviation security issues to the Honourable John Major in the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

Stuart Farson is an adjunct professor of political science at Simon Fraser University. He served as research director for the parliamentary committee that reviewed the *Canadian Security Intelligence Service Act* in 1989-90. He has worked with research institutes in Europe, North America and the Pacific Rim, testified before numerous parliamentary committees, and acted as an adviser to Canadian government and NATO task forces and workshops. He was an expert witness for the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar and in recent national security litigation involving port workers and the Marine Transportation Security Clearance Program. He is the author of numerous articles and book chapters on security and intelligence, and he co-edited *Security and Intelligence in a Changing World: New Perspectives for the 1990s, Intelligence Analysis and Assessment* and the *PSI Handbook of Global Security and Intelligence: National Approaches.*

This publication was produced under the direction of Mel Cappe, President, IRPP, and Wesley Wark, Fellow, IRPP. The manuscript was copy-edited by Barbara Czarnecki, proofreading was by Zofia Laubitz, production was by Chantal Létourneau, art direction was by Schumacher Design and printing was by AGL Graphiques.

IRPP
1470 Peel Street, Suite 200
Montreal, Quebec H3A 1T1
Telephone: 514-985-2461
Fax: 514-985-2559
E-mail: irpp@irpp.org
www.irpp.org

All *IRPP Choices* and *IRPP Policy Matters* are available for download at www.irpp.org

To cite this document:

Whitaker, Reg, and Stuart Farson. 2009. "Accountability in and for National Security." *IRPP Choices* 15 (9).

Security and Democracy / Sécurité et démocratie

Research Directors/Directeurs de recherche

Mel Cappe and/et Wesley Wark

This IRPP research program explores the complex challenges confronting Canada with regard to the post-9/11 security environment and its impact on domestic and international policies. The research addresses issues that are in many ways new to the country and to the formulation of Canadian national security policy, above all the threat posed by global, transnational terrorism. The program examines the interrelationships between new security demands and democratic norms, focusing in particular on the building blocks of a sound democratic model for national security, namely, effective intelligence; capable law enforcement; appropriate, stable laws; good governance; accountability; citizen engagement and public knowledge; emergency response capability; wise economic policy; and public-private-sector partnerships.

Ce programme de recherche s'intéresse aux défis de sécurité d'une grande complexité que le Canada doit relever depuis le 11 septembre, de même qu'à leur incidence sur nos politiques nationales et internationales. Il traitera d'enjeux souvent inédits pour notre pays en matière de sécurité nationale, notamment le terrorisme mondial et transnational. Le programme vise à analyser l'interrelation entre les nouvelles exigences de sécurité et les normes démocratiques, de manière à définir les éléments de base suivants : un modèle de sécurité nationale pleinement démocratique, notamment en matière de renseignement ; l'efficacité du maintien de l'ordre ; la stabilité et la légitimité des lois ; la gouvernance éclairée ; la responsabilisation ; l'engagement citoyen et l'information du public ; l'intervention d'urgence ; une politique économique avisée ; et les partenariats entre les secteurs public et privé.

Contents

Accountability in and for National Security

Reg Whitaker and Stuart Farson

Introduction

In this paper, we examine the complex system of accountability that applies to government departments and agencies responsible for Canada's national security.[1] Our objective is to identify and discuss both the process of accountability and the purposes underpinning it. We believe these purposes are primarily to protect the state's democratic fabric; to preserve and enhance its national interests; to ensure the safety of its citizenry; and to prevent the abuse of extraordinary intrusive or coercive powers. Questions of both the propriety and the efficacy of government departments and agencies therefore necessarily follow. In pursuing such questions, we hope to elaborate upon both the strengths and the weaknesses of the Canadian system. We intend to put forward recommendations that would enhance Canada's system of accountability without simultaneously hindering the operations of those involved in protecting Canada's national security.

Several conceptual difficulties need addressing. An initial caveat: accountability and national security are both contentious terms. While we explore various conceptions of accountability, we should acknowledge that what constitutes national security is itself debatable (Saltstone 1991, 36-54; Forcese 2006, 963-1000; Forcese 2008b, 3-13). The mere fact that a government claims something to be a matter of national security does not necessarily make it so. Such claims, in fact, may be vehicles for avoiding closer legislative watchfulness. On some occasions, they may be in direct conflict with other equally important concepts, such as the public interest. Such claims therefore deserve careful consideration.

Other contentious concepts requiring special elucidation include review and oversight, especially when independent bodies conduct such processes. Of the

IRPP Choices, Vol. 15, no. 9, September 2009

two, review is seen as scrutinizing institutional practices after the fact, and is therefore less likely to be perceived as politically contentious. Oversight, however, which is often associated with scrutiny beginning earlier and continuing after the fact, tends to be more problematic because it is seen as necessarily intruding upon executive systems of control and management, which are geared primarily to ensuring institutional efficacy and compliance with policy, regulations and law. Although after-the-fact review has generally been the preferred option in Canada for independent scrutiny, we find this preference neither desirable nor entirely logical when measured against the objectives for accountability in national security.

We argue that the debate over how best to scrutinize Canada's security and intelligence community has not fully considered the strategic intent of the various bodies and processes selected to effect accountability, nor has it adequately differentiated between their capabilities. In short, there has been an inadequate assessment of their effectiveness in terms of what they should and can accomplish. Thus, there are several important questions to ask of the institutions and procedures once they are in place, some necessarily on an ongoing basis. For example:

- To what extent do the various accountability procedures make the entire security and intelligence community understandable, transparent and public?
- Do the institutions have sufficient legal authority to conduct meaningful scrutiny of both institutions and practices? Are they limited in practice in the information that they receive or the people they can interview?
- How independent are the institutions involved and what is the likelihood of their being co-opted?
- Does the organizational culture of an institution limit its capacity to scrutinize effectively?
- Are the institutions limited to scrutinizing one organization or several?
- Are they interested in both propriety and efficacy?
- To whom do they report, and are their reports distributed in a timely fashion?
- Can they make those with executive responsibility account for their actions? Is the government obliged to respond to their reports within a set time frame?
- Can they effect change, and if so, how? For example, are their recommendations binding?
- Is there any institution or process that ensures all the various accountability components are doing their respective jobs effectively?

Governments have a broad choice of instruments when it comes to developing new policy, scrutinizing it in progress and evaluating it after the fact for transparency, legitimacy and public participation. We find that accountability has been sought for both propriety and efficacy, two different but interrelated criteria, which we discuss in more detail later. While after-the-fact reviews may be appropriate for investigating matters of impropriety, this does not negate the need for ensuring before the fact that institutions have appropriate policies and procedures in place to guarantee propriety. In the case of efficacy, both before-the-fact scrutiny and after-the-fact scrutiny may similarly be appropriate. Thus, we will insist upon widening the scope of the debate about how accountability should be understood to include the practices of both review and oversight.

From our perspective, while various forms of scrutiny processes exist in all three branches of government, they fall into three general categories. First, there are those that have only a propriety mandate. The commissioner for the Communications Security Establishment Canada, for example, has no legal authority to evaluate whether the agency is achieving its intelligence objectives. Second, certain commissions of inquiry have dealt mainly with matters of efficacy. Finally, institutions like Parliament and to a degree the Security Intelligence Review Committee (SIRC) arguably have an ongoing mandate to do both. In the latter regard, both the powers available and how they are exercised are crucial. Here it is important to draw distinctions between powers that are provided in law and those exercised in practice. Three dimensions are of importance here: (1) access in practice to documents and people; (2) the capacity to scrutinize bodies, to question responsible parties and to anticipate detailed and accurate responses from them; and (3) the process, timing, substance and independence of the reporting procedures.

In this paper, we will also show that bodies such as Parliament have considerable powers in law to access people, papers and records, but do not necessarily exercise these fully in practice. Similarly, we demonstrate that offices such as that of the inspector general of the Canadian Security Intelligence Service (CSIS), while having legal authority to see particular records, do not necessarily always have access to the people who control them, and thus cannot question the individuals responsible for those records. We will also point to the fact that the capacity to question those ultimately responsible for the control and management of an organization, which is fundamental to the process of accountability, differs considerably. For example,

Parliament, largely because of its committee system structure, the resources that committees command and the procedures that they follow, frequently fails to question witnesses adequately when they appear before its committees (Savoie 2008b, 302). While commissions of inquiry may do a better job in this regard, they sometimes fail to explore critically all the appropriate policy questions, arguably a matter for which parliamentarians may be better suited. Processes and organizational culture offer useful explanations for such eventualities. We will also indicate that bodies such as SIRC, while having the legal obligation to report on important issues in a timely fashion, sometimes – as with the Air India bombing – have failed to do so. Here the actual independence of the reporting bodies is important. The media, with restricted access, suffer few limitations on what they report, while official bodies, with relatively unrestricted access, often are constrained as to the details of what they may publicly disclose for legitimate reasons of national security.

The approach we take in this paper begins with an evaluation of the concept of accountability itself, discussing in the process such problems as secrecy and disclosure that may impede or enhance the practice. The analysis then adopts a historical approach to indicate how and when accountability procedures developed in Canada. We identify three periods with a view to showing that accountability constitutes an evolving but unfinished process. A summary of the key findings follows, along with our policy recommendations.

We should note at the outset, however, that some matters are covered more broadly than others. For example, there is much greater emphasis on external modes of scrutiny and accountability than on those operating internally: hence our distinction between accountability *in* and *for* national security. The reason for this should be obvious. External processes are more visible and better publicized than internal ones. Similarly, greater emphasis falls on organizations and intelligence practices that have been controversial than on those that have remained out of the spotlight. Thus, the roles of the CSIS and the Royal Canadian Mounted Police (RCMP) garner more attention than those of analytical bodies such as the International Assessment Staff (IAS) in the Privy Council Office (PCO) or the coordinating and policy roles of the PCO itself. We acknowledge that this emphasis is itself problematic, as it tends to focus attention on the workings of individual agencies rather than the security and intelligence community as a whole, a particularly important dimension when questions of overall efficacy are at stake.

We also acknowledge that this paper does not discuss the role of the media or that of academics and think tanks in making security and intelligence organizations more transparent and accountable in any discrete way. Each of these entities has played a significant part and deserves separate consideration. In addition to their media reportage, individual journalists have been responsible for numerous informative books – some groundbreaking – on various aspects of Canada's security and intelligence community (Campbell 2009). The academic community has been vibrant and growing, particularly since the establishment of the Canadian Association for Security and Intelligence Studies in 1985, with hundreds of articles and books now available. Political scientists, historians, legal scholars and criminologists are the most active but participants also come from other disciplines. More recently, think tanks have also become interested in the field, some devoting special issues of their journals,[2] others providing special reports (Cooper 2007).

The Concept of Accountability

Accountability may be defined in broad terms: A is accountable to B when A is obliged to inform B about A's actions (or inactions) and decisions, to justify them as appropriate and proper and, in the case of misconduct, to suffer sanction (Schedler 1999, 13–28). We will attempt to explore some of the complex dimensions of this concept later, but for now this broad definition will suffice. Accountability has particular reference to government and the control of political and administrative power, but may also be applied to corporate governance in the private sector and indeed to any organizational structure in which decisions affecting the public are regularly taken.

It is the consensus of many observers who have looked into this issue that accountability in the context of national security has to be understood as a particular case within the wider question of governmental accountability in liberal democracies. On the one hand, special rules must apply when considering accountability procedures for agencies tasked with protecting national security that may not always be

applied to many other agencies of government. In particular, there are special constraints on disclosure of information and limitations on the degree of transparency of operations that can be permitted. On the other hand, special protections against the misuse of the intrusive and coercive capacities that security and intelligence agencies have at their disposal deserve particular attention. Accountability procedures for national security must be uniquely designed for this specific purpose, and may not necessarily serve as models for wider accountability requirements.

Accountability as democratic buzzword

However distinct the policy issues may be, it cannot be mere coincidence that demands for greater accountability in national security have grown in recent years in parallel with the broader popularity of accountability as a democratic standard. Although there have always been specific national security issues and concerns that have driven the process of designing or improving accountability systems in this area, the broader context has informed and coloured public expectations, perhaps not always realistically.

Accountability has in recent years become a popular buzzword in liberal democracies, as an aspect of campaigns to democratize the political process. Like most buzzwords enjoying a popular vogue, the idea bears an unmistakable general thrust but lacks a consensus on a precise definition.

For many, the term implies simply an enhanced level of transparency in government. Elected officeholders and appointed officials should be held answerable to voters and taxpayers for their actions and their expenditure of tax dollars. When things go wrong, or are suspected of going wrong, there ought, it is widely believed, to be means available to check the process, identify problems, assign blame if required and initiate corrective action. Authorities, it is argued, should not have an untrammelled right to hide behind a cloak of official secrecy when the public interest is at stake.

In one sense, the demand for greater accountability is an extension of a democratization process begun long ago. In the nineteenth century, Canada's constitutional democratization process was driven by the struggle for responsible government, which meant requiring the executive to maintain the confidence of the elected legislature. By the latter half of the twentieth century, rising dissatisfaction with the limitations of legislative control of an increasingly large and complex administrative apparatus led to searches for new procedures of accountability that would both enhance the capacity of the legislative branch to keep a check on the executive and, to an important extent, establish more direct lines of accountability between the executive and the public. This process has accelerated since the 1960s, with populist campaigns emerging from both the right and the left of the political spectrum that have sought new ways to democratize the political system. Sometimes this has taken the form of attempting to transform political parties into more responsive instruments of popular will, attempts that have foundered on the realities of pluralistic trade-offs and compromises characteristic of democratic politics. More often, it has taken the form of new or improved institutional mechanisms to audit the actions of government. Thus, an institution such as the Office of the Auditor General (OAG), which reports to Parliament on the operations of the executive, has developed, especially under the current auditor general, Sheila Fraser, a popular following as a kind of tribune of the people uncovering waste and malfeasance in government. The same could be said for special commissions of inquiry set up to investigate scandals. The televised Gomery Commission hearings, for example, developed a surprisingly large and attentive audience in Quebec for hearings probing corruption and kickbacks in the sponsorship program.

In the 2004 and 2006 national elections, accountability, or lack thereof, was a leading campaign issue. The Liberal government of Paul Martin was battered by charges of corruption and cover-up and an alleged "culture of entitlement." The Conservatives came into office pledging to clean up government and make it more accountable. The new government, following a campaign promise, enacted the *Federal Accountability Act* as one of its leading priorities.[3] This legislation exemplifies the somewhat fuzzy meaning of accountability; despite its name, the Act does not define the concept, and includes within its scope several measures that have little apparent connection to accountability, as such.[4] It is as if the term *accountability* has such a good ring to it that it was deemed the most appropriate label for an omnibus administrative reform bill.

Ironically, some well-informed experts have been arguing that in practice accountability has actually been deteriorating in the face of the growing power of the Prime Minister and cabinet, despite the popular rhetoric.[5] In any event, there is little clear agreement on what accountability should actually mean, what practical measures will best improve it or even what the strategic intention of particular specific mechanisms

should be. Nor is there a clear consensus on what might constitute appropriate mechanisms for achieving greater accountability. Furthermore, there is little appreciation of the often unanticipated and sometimes perverse consequences of new accountability measures. The controversy that led to the *Federal Accountability Act* offers one example: following the public revelations of the sponsorship affair, the Martin government, in a failed pre-emptive strike, enacted a series of new controls and constraints on the public service. Together with some of the provisions of the *Federal Accountability Act*, these measures have had a damaging impact on governmental efficiency and the morale of public servants. Legitimate grant programs have become almost paralyzed with over-bureaucratization – all in the name of greater accountability.[6]

Accountabilities

Accountability processes can serve quite different objectives; these objectives can be met by different strategies. Thus, there is a need to examine the concept more analytically and strategically. There are some clear distinctions that can be made. Accountability may be controlling and/or explanatory (Marshall 1978, 51-65). Accountability as a control mechanism is exercised most often within organizations in a hierarchical power structure. Accountability as an explanatory process more often involves the cooperation of an organization with an external body that reviews or audits its performance. Accountabilities for control and for explanation should ideally work together. A working example is the external audit function, performed by an independent body such as the OAG, recommending changes in organizational procedures that are then effected internally. Scrutiny leads to explanation and thus informs control.[7]

Processes of accountability might seem to imply a relationship of power or influence over those held to account, whether by control or by cooperation. But accountability importantly offers legitimacy to those persons or organizations held accountable. By effectively managing the presentation of information about their activities, organizations can communicate a favourable image of themselves via their reviewers.[8] As a result, external review bodies are sometimes said to have been co-opted by the agencies they review (Johnson 2005, 72-3). This is not inevitable, but it is a frequent outcome of accountability in practice. Anyone designing new accountability procedures should remember the question "Who will watch the watchers?"

Examining accountability from the perspective of improving government performance, a former senior Ottawa public servant and student of public administration, David A. Good, cites three ways of looking at accountability from the inside, as it were (Good 2003, 166-73; Aucoin and Heintzman 2000, 43-53). Besides accountability for control, there is also accountability for assurance and accountability for learning.

Accountability for control means controlling the abuse and misuse of public authority as well as insisting upon administrative efficiency in the expenditure of public funds. Accountability for assurance, on the other hand, is concerned about providing assurance to Parliament and citizens that public authority and tax dollars have been used appropriately and ethically (this is close to the acquisition of legitimacy, discussed above). Accountability for learning means ways by which the assessment of performance becomes the stimulus for promoting improvement. Good cautions that each of these forms of accountability hides tensions and contradictions, especially when all three are pursued simultaneously by organizations. He concludes that "any single accountability perspective is partial, incomplete, and in competition with the others. It is by skilfully combining and balancing all three that we are likely to see the most progress" (2003, 179).

Another series of questions to be asked about accountability systems may be summarized as follows.

- Accountability *for what*?
  What part of an agency's mandate is it held accountable for; what precisely is the agency answerable for?
- Accountability *to whom*?
  To whom is the agency answerable? This apparently simple question may not have a simple response. There may be a diffuse set of offices or sites to which the agency answers, some for explanation, some for control, some for assurance, some for learning.
- Accountability *by whom*?
  Who actually carries out the review or audit? It may be an internal or an external process, or some combination. Public perception tends to be suspicious of internal review as lacking transparency. The most effective means of control are internal, but these may require unusual transparency for legitimation.
- Accountability *of whom*?
  At first glance, this may look like another take on "of what," but in practice it is a distinct question. For example, is the agency head held effectively

responsible and answerable for shortcomings found by auditors or reviewers, or is responsibility more diffusely spread through the organization?

- Accountability *when*?
  The question of timing may have very real consequences. From the point of view of an operational agency, accountability in the form of oversight over ongoing business is different from *ex post facto* review or audit. Yet even the latter may have operational consequences if officials alter their behaviour in expectation of the later findings of external review.

A central ambiguity in the institutionalization of accountability lies in its constitutional role in Westminster governmental systems, particularly with regard to Parliament. At issue here is the continued interplay between two crucially important constitutional conventions: accountability and ministerial responsibility. This has left an important problem unresolved, a potential conflict between ministerial responsibility and the accountability of appointed officials, which begs the question: Who is ultimately answerable? Historically, ministers of the Crown were considered to have a unique and the sole legal and political responsibility for an accounting to Parliament of all the actions and inactions of the personnel within their respective portfolios. However, as the complexity and size of government have grown in recent decades, so has the reluctance of ministers to take full responsibility for actions of their departments and officials, or at least to take responsibility to the extent of resignation in recognition of serious error. At the same time, governments have attempted to distinguish between matters of ministerial and bureaucratic responsibility. Initially, a division was drawn between issues of policy and those of administration; this was at best a divide that sometimes lacked clarity. More recently, however, there have been efforts to draw a distinction between accountability and answerability – the latter encompassing the role and responsibilities of senior bureaucrats – and to provide for designated persons as departmental accounting officers.[9] Such persons now have a legal obligation under the *Federal Accountability Act* to appear before parliamentary committees to answer questions on management practices, changing significantly in the process the relationship between senior bureaucrats and Parliament. While there may be some justification for a diminished level of direct ministerial responsibility for all the activities of very large and complex organizations, there has to be concern that strengthened procedures for administrative accountability may have the effect, intended or unintended, of effectively reducing ministerial responsibility and thus ministerial control. Thus, paradoxically, while statutory measures such as those making the director of CSIS responsible for the "management and control of the service under the direction of the Minister" may have originally been intended to enhance the accountability of the civil service to the minister, they may in the long run have made the minister less answerable to Parliament for aspects of the service's functions.

There is also the issue of the role of Parliament, *qua* Parliament, in relation to ensuring the responsibility of ministers and the accountability of the government in and to Parliament. In the case of the sponsorship affair, the Public Accounts Committee of the House (chaired by an opposition MP) held well-publicized hearings in parallel with the hearings of the Gomery Commission. In the case of the Mulroney/Schreiber affair, the House Committee on Access to Information, Privacy and Ethics (also chaired by an opposition member) called the two key witnesses to testify, before the special adviser appointed by the Prime Minister made his recommendation to the government on the terms of reference for a public inquiry. While Parliament is clearly within its rights and privileges to hold such hearings, any recommendations or findings it may make, in these or similar circumstances, rest in ambiguous relation to those of the findings of a public inquiry, especially when the Canadian Parliament has no say – as is the case in some jurisdictions – regarding the terms of reference of commissions of inquiry. The role of Parliament in accountability or responsibility in relation to the executive is an unresolved problem at the heart of the Westminster system. At its heart is a conflict in the roles parliamentarians perform. On the one hand, they are expected to follow party interests, attacking or defending the government according to the side of the House on which they sit. On the other, all parliamentarians have an obligation to pursue parliamentary interests on behalf of all Canadians by scrutinizing the activities of the executive branch, particularly concerning the expenditure of public funds and compliance with law and policy generally.

In short, despite the popular currency of the idea of accountability, there is no clear and unique definition of accountability that attracts a broad consensus, and no single form of accountability that obviously answers to the contemporary democratic demand. Perhaps it would be better to think of many accountabilities, operating in parallel beside one another, each

answering to different aspects of the questions of transparency and democratic control, each performing better or worse depending on its context, its design, the relative tractability of the issues on which it is brought to bear, and the organizational cultures of those performing the task.

Secrecy and accountability

Accountability and transparency seem to go hand in hand. Yet even in a liberal democracy, public administration is rarely public, in the sense of being transparent to the public eye. Much of the business of government necessarily takes place behind closed doors, just as much of the business of private corporations is kept securely out of the public eye. There are both good and bad reasons advanced for secrecy. It is the job of auditors and reviewers to expose bad reasons and cover-ups. By the same token, accountability must respect the legitimate grounds for secrecy, which may be desirable in the public interest, and must work within certain limits on transparency.

The first sociologist of bureaucratic organization, Max Weber, wrote that a high degree of secrecy is characteristic of all bureaucracy (Weber 1970, 233-4). According to a leading observer of British government, administrative secrecy is "Whitehall's cardinal virtue and dominant characteristic." He suggests that "secrecy is the bonding material which holds the rambling structure of central government together...Of all the rules of government, secrecy is the most sacred" (Hennessy 1990, 345-6). The Canadian political scientist Donald Savoie comments that "things are not much different in Canada...Secrecy and confidentiality have also permeated government operations in Canada" (2003, 44).

One of the rationales for secrecy is the highly competitive and partisan nature of the parliamentary process. Information about government is used by the opposition as the source of criticism. In practice, governments often try to minimize their exposure to political risk by managing the presentation of information in ways that enhance their political credibility. Government and opposition are only fulfilling their respective roles in a competitive democratic environment, but the result is that secrecy is the rule, while disclosure is the exception, either forced or managed, as the case may be.

It has always been a principle of the Westminster system of government that cabinet deliberations remain strictly confidential, thus allowing individual ministers to speak their minds freely. As a result, "cabinet confidences," which include not only cabinet minutes and decisions but also documents submitted to cabinet by the senior public service,[10] are excluded from the *Access to Information Act* for at least 20 years.[11] Of course, there are also legal and ethical reasons for maintaining forms of administrative secrecy. The larger government has become, the more its operations penetrate and influence society, the greater the need to maintain secrecy about its plans, lest private interests gain financial or competitive advantage from "inside information." Thus, there are strict requirements for secrecy surrounding the preparation of both budgets with tax implications and regulatory instruments for the private sector.

Secrecy in government may be inevitable, but the acceptable degrees and limits of secrecy are often issues of controversy. This is especially the case where accountability is in question. The administrative requirements of confidentiality and the need for relative transparency in holding governments accountable are in persistent tension with each other. Accountability fails when secrecy is deliberately employed to cover up incompetence or wrongdoing. Yet an accountability mechanism that fails to respect a legitimate or practical reason for secrecy will be unworkable. It should be noted that not all accountability systems necessarily require full public disclosure, especially where political sanctions are not required. Successful accountability procedures must negotiate a delicate path between secrecy and transparency, which is easier said than done.

Problems of accountability in national security

The secrecy/transparency problem is magnified when accountability is applied to national security issues and practices. The various organizations making up Canada's security and intelligence community have special and necessary requirements for secrecy that exceed the requirements for secrecy in other areas of government operations. Mechanisms appropriate to ordinary forms of public administration are usually inappropriate in a context in which secrecy is the general operational rule, to which exceptions are allowed only sparingly, not to speak of grudgingly. National security operations are often opaque not just to the public but to other public servants who are not part of the security apparatus, and this privileged access to secrecy is jealously guarded. Based on experience elsewhere, public expectations of accountability in national security are relatively high, but it is a complex task

to devise, deliver and administer appropriate mechanisms that do not undermine the requisite opacity within which national security agencies operate. It is nonetheless the case that the specific requirements for secrecy must be taken fully into account in designing any accountability system in this area. We can look at these specific requirements in turn.

Secrecy of sources

The police, the military and intelligence agencies have always relied upon human sources of intelligence. They have been adamant that the identities of their sources, and the identities of agents operating under cover, must be fully protected from public disclosure. The ironclad promise of anonymity of sources is crucial to recruitment and retention: whatever the motive for cooperating (which may range from idealism to coercion to financial incentives, or mixtures thereof), potential human sources must be assured that their double identities will never be revealed. The moment the identity of a source is disclosed, the usefulness of that source is terminated. In many cases, as with the penetration of violent organizations, the protection of the identity of a source may be literally a matter of life or death. Moreover, the disclosure of one source may jeopardize the ability to recruit others.

The *Canadian Security Intelligence Service Act* (*CSIS Act*) makes it a criminal offence punishable by up to five years' imprisonment for an official or former official to make an unauthorized disclosure of the identity of "a confidential source of information or assistance" to CSIS or "any person who is or was an employee engaged in covert operational activities of the Service."[12] The *Access to Information Act* contains exemptions for information that "would reveal the identity of a confidential source of information" in criminal law enforcement investigations, or "any record requested under this Act that contains information the disclosure of which could reasonably be expected to threaten the safety of individuals."[13]

The disclosure of confidential sources has sometimes been an issue when deciding whether to initiate criminal prosecution in national security cases that rest on the testimony of confidential sources.[14] Part 3 of the *Anti-terrorism Act* contains a number of amendments to the *Canada Evidence Act*[15] seeking to protect against the disclosure in open court of the identities of sources in anti-terrorist cases.[16]

Secrecy of investigative methods and tradecraft

Equally important to national security agencies is the protection of information about their methods of investigation, including technical means of intrusive surveillance. Since the targets of security surveillance and criminal investigations constitute covert or concealed threats to the security of Canada, the methods used to identify and assess these threats and initiate criminal prosecutions must necessarily be protected from disclosure, because any such information could assist those targeted to evade detection. Investigative methods may encompass a wide range of matters, from targeting to budgeting of resources, from operational technology to the "tradecraft" of the agency's operatives (the accumulated experience and culture of how they go about their business).

As with human sources, investigative methods are protected against disclosure under the *Access to Information Act* and *Privacy Act*, and may also be blocked from disclosure in court under the strengthened evidence provisions of the *Anti-terrorism Act*.

Secrecy of information received in confidence from abroad

A major reason for secrecy is the reliance by Canada's various national security agencies on information received in confidence from foreign governments and their agencies, or from international organizations. A significant proportion of the intelligence on which Canada relies to assess threats to Canadian security results from intelligence exchanges and information sharing with cooperating agencies in friendly countries. Much of the intelligence that Canada receives is designated as confidential and released only on the guarantee that it will not be publicly revealed. In some cases, the intelligence is accompanied by caveats limiting access to the recipient agency only; the latter is expected to restrict circulation even to its allied agencies. Canada, in turn, shares its intelligence with cooperating foreign agencies on the same basis of confidentiality. Breaches of these arrangements could result in a breakdown of the networks of intelligence exchange, which could seriously damage the effectiveness of security and law enforcement cooperation in Canada and abroad. Thus, Canadian agencies are insistent that confidentiality regarding all information received from allied and cooperating agencies must be protected from unauthorized disclosure.

A number of legal guarantees against unauthorized disclosure of material received in confidence are embedded in various Canadian statutes, including the new *Security of Information Act*, and in evidentiary

procedures in Canadian courts when disclosure could be considered injurious to the conduct of international relations.

Accountability and disclosure

Even if the special case for secrecy is granted, it is no longer considered acceptable that secret agencies should be able to act, in effect, as sole judges in their own cases in defining what must remain secret and what may be disclosed. Disclosure decisions are normally subject to judicial review, even if it is necessary to hold *ex parte* proceedings, where secret material is reviewed in camera. Accountability procedures for national security typically operate with some mixture of publicity and secrecy. Review bodies have access to information that cannot be disclosed, or even in some cases explicitly referenced in public, but this need not deter them from reporting their findings publicly, with as much indication concerning confidential material as can be reasonably summarized. Occasionally, disputes over disclosures between agencies and those bodies reviewing their activities may require adjudication by the Federal Court. But no longer can the requirements of secrecy be taken as a bar to external accountability.

Secrecy, moreover, is not merely a matter of insiders versus outsiders. Within the executive branch of government, those directly involved in national security have privileged access to secrets not generally available to other departments and agencies. To the extent that they can withhold information from other parts of the executive, they may be less accountable. Even within security and intelligence agencies, there are well-known practices of compartmentalization and the "need to know" principle that limit the transparency of operations to colleagues, let alone outsiders. This is a problem that only accentuates the need for accountability within government as well as from the outside.[17]

It should be noted that while individual MPs and senators are limited, Parliament as a body is not restricted in its actions, except by legislation that specifically binds the Crown. Thus, for example, it is not limited in its access to records by the *Access to Information Act*, the *Security of Information Act* or the *Privacy Act*. In fact, Standing Order 108 of the House of Commons and a similar Order of the Senate expressly provide the two houses, and their committees through delegation, with the capacity to call for such "persons, papers and records" as they choose, thus providing a quintessential enabling aspect of political accountability. Individuals who fail to comply are liable to be held in contempt of Parliament. In practice, however, government documents and personnel have tended to be made available at the discretion of the government because the executive is normally able to exercise its majority. While for the most part parliamentarians have tended to demonstrate a certain deference to government when faced with a disinclination to release information or to make people available, there have been notable exceptions to this general rule.[18] It should be noted that in minority Parliaments – such as have been in place since 2004 – there is no such capacity on the part of government to thwart the intent of Standing Order 108. Nor has the Liberal majority in the Senate used its powers to force the disclosure of information from the current Conservative government.

Once in Parliament, members are free to use such information as they see fit. Parliament's record for keeping its own documents confidential is not particularly good. There have, for example, been numerous leaks of committee reports before they were tabled in the House. With regard to the release of information provided during in camera hearings, which is meant to remain private, Parliament's record is better, but not foolproof.[19] Thus, the possibility of sensitive information becoming public through Parliament is potentially a matter of genuine concern for intelligence officials.

National security and law enforcement

The need to maintain high levels of secrecy in national security matters is not the only barrier to accountability. Threats to national security pose an intelligence problem to governments charged with the responsibility for maintaining public safety and promoting the national interest. National security agencies collect information and assess such threats, sometimes employing intrusive surveillance and other extraordinary powers to do so. But security threats also pose a law enforcement problem, particularly where criminal investigations and criminal prosecutions may be undertaken.

In Canada, before 1984, both security intelligence assessments and national security criminal investigations were the responsibility of the RCMP. Following the recommendations of the McDonald Commission (Commission of Inquiry concerning Certain Activities of the Royal Canadian Mounted Police) in 1981, the government accepted that this combination of responsibilities in a single policing agency was inappropriate.

Consequently in 1984, Parliament passed the *Canadian Security Intelligence Service Act*, creating CSIS as a service without police powers, along with the *Security Offences Act*,[20] which specifies law enforcement responsibilities for the RCMP regarding national security offences. This institutional division of roles for national security is one that has long been practised in the United Kingdom, where the Security Service, known as MI-5, is separated from the various Special Branches of UK police forces, which alone have law enforcement responsibilities. However, in the United States, the Federal Bureau of Investigation (FBI) still combines both security intelligence and national security law enforcement within the same agency.

Whatever the institutional arrangement, the distinction between security intelligence and law enforcement is important in determining appropriate mechanisms of accountability. In regard to law enforcement, Canada retains the well-known principle of police independence, requiring an arm's-length relationship between external political control and decisions to initiate and/or to halt criminal investigations, as well as to prosecute. This has been widely accepted as a necessary safeguard against a government that might abuse its law enforcement powers by arbitrarily directing them at its opponents.

In regard to security intelligence, direct political control – as opposed to accountability – of agencies engaged in sensitive national security threat assessments is generally regarded as not only desirable but necessary. In the absence of such control in the form of ministerial responsibility, security intelligence agencies with their extraordinary and intrusive powers might be seen as a potentially unchecked threat not only to the rights and liberties of citizens, but even to the elected government of the day.

Where the two functions overlap, especially when they overlap within the same agency, there is inevitable tension between the need for an arm's-length relationship and the need for direct control. In the early 1980s, Parliament prescribed different accountability procedures for CSIS and the RCMP, reflecting their different roles and the different principles of governance surrounding these roles. The overlap of functions must be fully taken into account in devising an effective accountability system for a law enforcement agency involved with national security issues.

Accountability and oversight

Accountability is sometimes viewed in conjunction with or in contrast to oversight. These concepts overlap but are analytically distinct. Both are essential for developing and maintaining public trust in government and its institutions. Both are processes that are still evolving in meaning and in practice, and each has different historical origins.

Accountability had its origins as a constitutional convention in Westminster systems of government (where the executive and the legislature are fused). It is directly related to another constitutional convention covering the notion of ministerial responsibility. In this sense, it relates to the obligation of ministers to account for the actions and inactions of the departments and agencies within their respective portfolios in and to Parliament. The responsibility is both a political one and a legal one. Parliament has certain powers and privileges it can use to ensure that this accounting occurs.[21]

As already indicated, accountability has more recently taken on broader meanings. These imply that government actions should be as transparent as possible and that there should be public input into the policy process. Thus, the process of accountability may encompass measures that are practised by the formal arms of government as well as by other elements of civil society (academic writers, the media, think-tank researchers, nongovernmental organizations). Many of these conceptual frameworks and practices have been developed in the US.

The notion of oversight had its origins in the US. There it refers to the scrutiny of the executive branch of government by the legislative and judicial branches. In the congressional sense, oversight takes many forms and serves several different objectives: appropriation, authorization, scrutiny of legislation, fact-finding, review of governmental practice and the evaluation of best practices.

Oversight has often been misconstrued outside the US as necessarily involving control over agencies, departments and government practices (Public Safety Canada 2004). Oversight sometimes applies controls, but this is not necessarily always the case. This has led to arguments (particularly in Westminster systems) that favour after-the-fact reviews rather than scrutiny during or before the fact. It should be noted that the scrutiny of government departments, agencies and programs for performance and capability necessarily demands some degree of before-the-fact scrutiny (Light 1993, 14).

Twenty-five years ago the term *oversight* was seldom used outside the US. When it was employed to refer to other governmental systems, critics referred to it as belonging to the congressional system and not applica-

ble elsewhere, particularly to the Westminster model. Two arguments buttressed this position when applied to Canada. One was the notion of after-the-fact review. The other was that oversight necessarily implied a controlling function. Such arguments have been repeated in recent times – albeit in modified form – but without solid substantiation. Consequently, their basic premises deserve a critical examination in three important respects.

First, American congressional experts themselves do not necessarily agree that oversight always implies a controlling function on governmental practice by Congress (Aberbach 1990, 217-9). As we have shown with the concept of accountability, congressional oversight serves many functions. In some instances, such activities do lead Congress to impose certain controls through its more independent capacity to legislate, and through its ability to tighten funding. But, equally, in others it does not do so. The responsibilities of the permanent select committees on intelligence are a case in point. Thus, congressional experts prefer to perceive oversight in less dramatic terms as scrutiny of government action.

Second, scrutiny of government action is now practised by a variety of government organizations, representing all three branches of government. Within the administration such scrutiny is provided by various inspectors general who form part of the individual departments and agencies as well as the various advisory bodies that are directly available to the president. To these must be added the various congressional committees as well as funded and staffed bodies such as the Government Accountability Office and the Congressional Research Service, which report directly to Congress, and the role performed by the judicial branch both in hearing cases brought before the courts and in authorizing or rejecting warrant applications. These bodies, it should be noted, vary considerably not only in the powers and access they have available but also in the degree of control and influence they can exert on those actually responsible for the agencies and structures involved.

Third, the term oversight is now widely used across a full range of governmental systems, including those of the Westminster model, not just the congressional system. Such usage, like that of American experts, seldom implies more than scrutiny, and it is in this sense that we would employ it here. We would also argue that scrutiny by such review and oversight bodies is a necessary precursor to the reports they may issue and hence to the accounts that those politically and legally responsible for the control and management of the security and intelligence community may eventually have to provide.

The term oversight is now used broadly in democracies (old and new) to encompass the various processes by which government action is scrutinized. It is now often used to encapsulate the entire process by which bodies are scrutinized and made transparent. The process of making something transparent ultimately depends on having the capacity to ask pertinent questions. The mere fact that the executive has an obligation to provide an account does not in and of itself make something transparent. The account may not be sufficiently detailed, and may even be misleading or obfuscating. You have to know what to ask. To know what to ask, in many respects, depends on the breadth of one's capacity to scrutinize government actions.[22]

In the end, much comes down to the question of public trust. When governments impose new security procedures that have serious potential consequences for individual rights and liberties and insist that these procedures are necessary to combat new heightened threat levels, the public needs to believe not only that the governmental analysis is accurate, and that infringements on rights and liberties are warranted under the circumstances, but also that the governmental organizations charged with dealing with the heightened threats are up to the task. Public trust in the intelligence capacity of governments has been shaken by the failure to anticipate and prevent the 9/11 attacks, but also by the misuse and abuse of intelligence by the American and British governments to justify the unsanctioned invasion of Iraq in 2003, a policy decision now widely understood as constituting a major fiasco. One senior Canadian intelligence official has stated confidentially that the politicization of intelligence over the Iraq War has done serious damage to the "intelligence brand." These intelligence failures and their political consequences impose a heavy burden on those attempting to restore public trust. This burden does suggest a greater emphasis on oversight, as opposed to *ex post facto* review.

Another important dimension of good governance concerns the issues of unintended consequences. Normally, greater transparency is thought to make for more effective and efficient processes of government. In certain areas of government – national security may be one – greater levels of review and oversight may in practice detract from efficiency by imposing undue burdens on management. Similarly,

more detailed accountability may lessen the effectiveness of the agencies if aspects of tradecraft are revealed. But while such dangers may be present, a cautionary note is nevertheless in order here. Intelligence bureaucrats in the US have sometimes sought to undermine accountability systems by arguing that additional scrutiny would lead to "micromanagement."

Historical Map of National Security Accountability

History to 1970

National security activities of the federal government, and in some cases of provincial governments, have a long history going back to the early years of Confederation in the late nineteenth century. Perceived threats were posed by violent Fenian Irish and Sikh groups before the First World War, by Communist and Bolshevik movements after the Russian Revolution in 1917 and by fascist and Nazi movements in the 1930s. More controversially, trade unions, students, citizens' associations and advocacy groups were sometimes targeted by the authorities as threats to Canadian security. In two world wars, there were alarms about enemy "fifth columnists" among immigrant communities; a number of their members were identified and interned, their organizations were banned, and censorship was imposed on them. The most notorious case was the forcible relocation of the entire Japanese-Canadian population of the West Coast to camps in the interior (Adachi 1976), an act for which the Canadian government later apologized and provided some financial compensation.[23]

In 1945–46, the defection of the Soviet cipher clerk Igor Gouzenko with documentary evidence of a Soviet spy ring operating in Canada was an important incident in the emerging Cold War between the wartime allies (Knight 2005). A secret order-in-council under the *War Measures Act* authorized the detention and interrogation of a number of suspects, without benefit of legal counsel. The Taschereau-Kellock Commission took secret evidence and published a report (Royal Commission to Investigate the Communication of Secret and Confidential Information to Agents of a Foreign Power 1946) in which some two dozen persons were named as betraying their country on behalf of a foreign power, even though only about half of those named were ever subsequently convicted of espionage or related offences in a court of law. In the aftermath of the Gouzenko affair, following the recommendations of the royal commission, the government of Canada constructed a peacetime national security state (Whitaker and Marcuse 1994), with screening of public servants and later of immigrants and citizenship applicants, and an extensive domestic surveillance operation by the RCMP Security Service that by the latter stages of the Cold War had accumulated dossiers on some 800,000 individuals and organizations (Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police 1981, 1:518).[24]

Despite grounds for concern about the rights and liberties of citizens in the face of this "political policing" of Canadian civil society, and despite occasional public protests, it is remarkable how slowly proposals were gathered for the establishment of mechanisms to make the operations of the secret state more democratically accountable. Until the late 1960s, Canadians by and large appeared to accept that national security agencies should work in secret, unchecked by any scrutiny outside the executive of the efficacy or propriety of their operations. Debates over national security during the two world wars and the early Cold War years were relatively consensual and bipartisan. It was only in the 1960s that the first serious stirrings of concern about a lack of accountability appeared. In 1965, two security-related scandals burst into public view as partisan political issues. The firing of a sick and dying Vancouver postal worker because he was suspected of being a Soviet spy caused a public outcry. Then the Gerda Munsinger affair implicated two cabinet ministers from the previous Progressive Conservative government in a relationship with a woman believed to have possible connections to Soviet espionage. Under considerable pressure from Parliament and the press, Prime Minister Lester Pearson called two separate commissions of inquiry to investigate these affairs – the Commission of Inquiry into Complaints made by George Victor Spencer and the Commission of Inquiry into Matters Relating to One Gerda Munsinger, which both reported in 1966 – and then followed these up with the Royal Commission on Security, with a wider mandate to develop policy. The terms of reference for this latter inquiry under M.W. Mackenzie were to "examine the operations of Canada's security procedures with a view to ascertaining, firstly, whether they were adequate for the protection of the state against subversive action and, secondly, whether they suffi-

ciently protect the rights of private individuals in any investigations which are made under existing procedures"[25] – in short, to ascertain both the efficacy and the propriety of security operations.

The Mackenzie Commission reported in 1969. While it was grounded in a somewhat uncritical Cold War mindset, the commission did make the first official recommendation for a formal accountability mechanism for the Security Service: a Security Review Board nominated by the governor-in-council, but "independent of any government department or agency." The board's main job would have been to hear appeals from public servants, immigrants and citizenship applicants denied security clearance. The board would also have received periodic reports from the head of the Security Service and would have had "authority to draw to the attention of the Prime Minister any matter it considers appropriate," a clear indication that Mackenzie considered accountability only in relation to the executive. No reference was made to accountability to Parliament, the courts or the public. Significantly, Mackenzie recommended that the Security Service be detached from the RCMP and reformed as a "new civilian non-police agency...quite separate from the RCMP...without law enforcement powers" (Royal Commission on Security 1969, 109, 110, 105). The status of the Security Service as a branch of the police force was seen as an obstacle to developing accountability, in part due to concerns regarding "police independence." The Mackenzie Commission tried to avoid this problem by linking "civilianization" of the Security Service to an accountability system for a new body without law enforcement powers. Neither recommendation, however, was implemented at the time, although the government did appoint John Starnes as the first civilian director of the RCMP Security Service, a recommendation that Mackenzie had made.[26] It seems that there was at this time insufficient public and political pressure on government to force any radical change in national security practice.[27] This first tentative consideration of change did, however, strike one note that has continued down to today: usually only public scandals and serious failures surrounding national security activities force government to consider accountability for propriety. The response is to initiate special inquiries that make policy reform recommendations.

Crisis of the 1970s and 1980s: from McDonald to the *CSIS Act*

The decade and a half that followed the Mackenzie Commission carried the scandal-inquiry-reform dynamic much further, ultimately leading to a major innovation in national security accountability. The key difference from the earlier period was the partial refocusing of domestic security away from the old Cold War Soviet "fifth column" threat to the targeting of a new internal made-in-Canada threat from violent Quebec separatists. In October 1970, hostage taking and political assassination by the Front de libération du Québec were met by the peacetime invocation of the *War Measures Act* against an "apprehended insurrection," detention without charge and without counsel of numerous suspects, censorship of the media and what amounted to martial law on the streets of Montreal.

Through the 1970s, there followed an unprecedented intervention by police and security authorities in Quebec against suspected separatists, unfortunately not always making clear distinctions between violent terrorist groups and legitimate *indépendantiste* groups like the Parti Québécois that may have represented a threat to national unity, but not to national security. New Left and peace movements, mainly independent of Communist influence, were also targeted outside Quebec. Excessive, invasive and sometimes illegal actions by both federal and provincial police later led to a series of commissions of inquiry at both the federal and provincial levels.[28] Although most Canadians opposed Quebec secession, the intrusive intervention by "secret police" in the political activities of Canadians unconnected to hostile foreign powers raised questions about democracy and the rule of law that seemed to demand structural reform and accountability of national security operations.

Pushed by provincial, especially Quebec, disquiet, and by a series of embarrassing media revelations of unlawful if not scandalous RCMP activities, the federal government was forced reluctantly to appoint a special commission of inquiry into actions of the RCMP not authorized by law. The terms of reference for the McDonald Commission noted that "public support" for the RCMP's national security operations was "dependent on trust in the policies and procedures governing its activities." The maintenance of that trust required a full investigation of the extent of unlawful activities and recommendations by the commissioners on the necessity and desirability of legislative and institutional changes to the governance of national security.[29]

McDonald Commission

In 1981, the McDonald Commission recommended a new institutional architecture to achieve a greater

degree of accountability and control over the RCMP Security Service. This was achieved by balancing the state's obligation to preserve civil liberties with its duty to protect and enhance national security – a balance captured in the title of the commission's second report, *Freedom and Security under the Law*. Its most significant recommendation was to separate the Security Service from the RCMP and reconstitute it as a civilian agency without law enforcement powers. In the changed political context of the time,[30] McDonald's civilianization proposal, unlike Mackenzie's earlier such recommendation, was implemented with the passage of the *Canadian Security Intelligence Service Act* in 1984. The *CSIS Act* mandated several new accountability procedures broadly inspired by McDonald, but its provisions occasionally departed – in some cases significantly – from McDonald's recommendations.

McDonald drew a clear distinction between accountability as control and accountability as explanation, the former taking the form of internal governmental direction, the latter the form of external or independent review. Both were to be grounded in statutory forms that would express the will of Parliament. The major elements of accountability for the proposed new civilian agency were as follows (Farson 1991b, 155-85).

Internal controls

While overall security policy and priorities were the responsibility of the cabinet, and while the "special" responsibilities of the prime minister in overseeing national security were recognized, McDonald affirmed that the solicitor general should be the minister directly responsible for the Security Service. The deputy solicitor general would be the minister's deputy in respect to all aspects of direction and control of the agency. McDonald insisted accountability must be ensured by an effective system of communications, within the agency and between the agency and the deputy solicitor general, "to ensure that the Minister is informed of all those activities which raise questions of legality or propriety" (Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police 1981, 842). The commissioners also recommended an effective system of financial control by the Treasury Board and the auditor general.

External review

McDonald was concerned that a joint parliamentary committee on security and intelligence should be able to examine the activities of the agency in camera. In addition, an Advisory Council on Security and Intelligence would assist the minister, cabinet and Parliament in "assessing the legality, propriety, and effectiveness" of the agency. Although lacking executive powers, it would have an "investigating capacity," and report its findings to the minister, and as well submit annual reports to the parliamentary committee. There would also be a Security Appeals Tribunal to consider appeals regarding security clearance decisions, with its advice provided to cabinet.

Judicial oversight and control

McDonald uncovered evidence that the RCMP had extensively employed intrusive surveillance techniques ("wiretaps") not authorized by law.[31] The commissioners recommended that applications for intrusive surveillance be submitted to a judge of the Federal Court for specific approval.

Parliament and public

Importantly, McDonald recommended that a joint parliamentary committee on security and intelligence should be empowered to examine national security activities in camera and in secret. Although this would, to some degree, situate the parliamentarians "inside the loop," McDonald saw this window as offering the opportunity for greater transparency. Ministers and parliamentarians should "endeavour to provide the public with all information possible about the security of Canada, the threats to it and steps taken to counter those threats." A more informed public would be better able to understand national security issues (Commission of Inquiry concerning Certain Activities of the Royal Canadian Mounted Police 1981, 843).

Ironically, while this recommendation for a parliamentary committee would be ignored, Parliament actually played a key role in the implementation of the main thrust of the McDonald plan for national security reform. Consequently, we now turn to a brief excursus on the role of Parliament in national security, a rather ambiguous if not convoluted story.

Parliament in the Canadian Westminster system

The *British North America Act* of 1867 passed on to the Parliament of Canada all those powers, privileges and immunities that were enjoyed by the parliamentarians at Westminster, including the right to remake any law it chose, and the stipulation that Parliament is not bound by any law that does not specifically bind the Crown.[32] While the privileges and immunities are still today enjoyed by individual members of Canada's Parliament,

the powers rest with Parliament as a whole, not with individual members, and must routinely be delegated to committees. Two are of particular importance when it comes to making the government of the day account for its actions and to effecting control over government action. The power under Standing Order 108 to call for "persons, papers and records," even when its use is only threatened, is an invaluable and powerful investigatory tool that, when backstopped by the capacity to hold individuals in contempt for non-compliance and the requirement to testify under oath, is crucial to the process of political accountability. Similarly, the expenditure of public funds cannot be continued without the formal consent of Parliament. Thus, by withholding such approval, or even raising the threat, Parliament retains a measure of control over government policies and programs.

During the first hundred years or so of its existence, Canada developed a variety of instruments from which governments could choose to investigate, inquire into, review, make transparent and generally scrutinize its policies, practices and administrative procedures. Among these tools were departmental and interdepartmental studies, task forces, regulatory and advisory agencies, parliamentary committees and commissions of inquiry, each with various subsets. These instruments varied considerably in their investigatory capacities and powers, their independence from the executive branch, their capacity to make things publicly transparent and their ability to hold people responsible for their actions, to effect reforms and to sanction wrongdoing.

By the middle of the twentieth century, Canadian government had expanded considerably and had become much more complex. To meet such new complexities, the organization of parliamentary business more and more reflected the departmental structure of the executive branch of government, especially in terms of committee work. The responsibility of individual standing committees to monitor and review governmental activities would normally work well as long as departmental responsibilities were entirely discrete and each committee's remit did not overlap with that of others. However, the normal committee structure would prove less effective where policies and programs tended to run across the gamut of government and be led and coordinated by a central agency, such as the Privy Council Office. The administration of security and intelligence matters constituted one such area of government, where responsibilities crossed departmental structures and where the Privy Council Office played a lead role in many dimensions. When coupled with the requirements of secrecy that these functions of government demanded, they would clearly prove to pose unique problems for parliamentary scrutiny. In addition, the adoption of the Canadian Bill of Rights had placed a new emphasis on the rights of individual citizens. While this meant new responsibilities for the minister of justice, who was required to ensure that all legislation was in accordance with the Act, it also implied the need for additional bodies to scrutinize particular aspects of government from the perspective of the public interest and to handle public complaints. To this end various ombuds-like offices were established to consider such matters as official languages, human rights, privacy, access to information and public complaints against the RCMP (Farson 2000, 225-58).

In 1982, Canada continued its progress toward becoming a full-fledged "constitutional democracy" when it patriated its constitution from Britain. With the entrenchment of the Charter of Rights and Freedoms as a central piece of this document, Parliament now found its supremacy less absolute in the federal sphere than hitherto. In the years that followed, certain legislation adopted by Parliament would be struck down for being unconstitutional. Similarly, regulations developed as a consequence of such enabling legislation would have to be even more closely scrutinized, both before promulgation by the executive branch and various independent bodies – such as the Office of the Privacy Commissioner – and subsequently by the Joint Committee of Parliament on the Scrutiny of Regulations. And its work as a scrutinizer of government action was augmented by review bodies sometimes depicted as parliamentary "surrogates."

Parliament and national security

Prior to the *CSIS Act* of 1984, the introduction of new or restructured components of Canada's intelligence community had been handled by executive order without involving Parliament.[33] Such matters as did come before Parliament were generally given short shrift (Franks 1980). As a consequence, the vast majority of parliamentarians knew little about Canada's secret world and had scant expertise in this important aspect of governance. Furthermore, despite their efforts during the 1970s to pose questions about the impropriety of RCMP Security Service activities, they were often rebuffed, being told either that matters could not be discussed publicly for reasons of national security or that matters were *sub judice*.[34]

The first occasion on which the Canadian Parliament provided any detailed study of national security matters was over the *CSIS Act*. The way in which the government introduced the legislation was unusual. Instead of tabling it in the House of Commons, the government sent its bill to the Senate, where a special committee, consisting of only Liberal and Progressive Conservative members, was established to consider it. Also surprising was the choice of the person to head the committee. Immediately before becoming a senator, Michael Pitfield had been the cabinet secretary, Canada's most senior civil servant. It had been under his watch that the recommendations of the McDonald Commission had been evaluated and the legislation drafted. If the government anticipated a free ride, it was mistaken, because the draft bill came up against considerable criticism in the Senate. As a result, the government allowed the Bill to die and introduced a new one incorporating most of the Senate's recommendations. Though it was debated at length in the Commons, where New Democratic Party members opposed it strenuously, no significant amendments were subsequently accepted by the government.

It is important to note that the Senate's report expressed a particularly negative view about Parliament's capacity to play a major role in the scrutiny of Canada's intelligence community. On this point, it stated a view that would find the support of government for at least 20 years:

> It has been submitted to the Committee that the operations of CSIS should be subject to the scrutiny of a special parliamentary committee which would have much the same powers as the SIRC. The McDonald Commission also recommended the establishment of such a committee. We agree that, ideally, such a committee would be of benefit. But there are many practical difficulties involved. A parliamentary committee in many respects would likely duplicate SIRC's efforts. Further parliamentary committees are notoriously subject to the vagaries of time, changes in membership and overwork. There is also the problem of maintaining the security of information. This has the possibility of partisan motivations in some members, but it also refers to the general question of whether that type of committee can maintain the requisite confidentiality by reason of the nature of its proceedings. In view of these considerations, the Committee believes it would not be advisable to establish a parliamentary committee with special access to CSIS operations and information. (Senate Special Committee on the Canadian Security Intelligence Service 1983, 31-2)

While the special committee was correct in pointing to the difficulties of time management, the frequent changes of membership of Commons committees and the overwork of many MPs, its suggestion that MPs could not be trusted either to protect the classified information or to keep their proceedings confidential begged for more detailed thought concerning alternative options and procedures. So too did its view that a parliamentary committee would have similar powers to the Security Intelligence Review Committee (SIRC). The McDonald Commission, for example, had not only envisaged a complementary role – not an alternative one – to SIRC regarding CSIS, but had foreseen the need for a parliamentary committee that would have had a much broader remit, one that would have encompassed the role of the various members of the intelligence community as a whole. In addition, there was no discussion concerning the possible benefits that a parliamentary committee might bring to the table, such as the capacity to bring resource deficiencies to the attention of the executive, to speak publicly on behalf of an intelligence agency when wrongly maligned in the press or to develop a knowledge base and degree of expertise for future ministers.

The special committee's concerns over partisanship also needed to be examined in more detail. While it is true that some committees demonstrate a high degree of partisanship, it would be wrong to assume that all committees do. Furthermore, there are often good reasons why such partisanship is exhibited, not the least because there are often genuine political differences as to how to proceed with policy initiatives. Unfortunately, senior bureaucrats sometimes become the targets of such partisanship, especially when committee members do not receive detailed responses to questions.[35] In part, this arises from a lack of clarity as to where the line should be drawn between policy, a matter for which ministers alone have responsibility, and administration, an area about which bureaucrats can respond to committees. There are also examples of committees working very harmoniously. Here the work a committee conducts in private, which is frequently less evident and often less accessible than that of the executive branch (the latter being subject to the *Access to Information Act* while private parliamentary committee business is not), is as important as its public hearings. Such was the case with the 1989-90 House of Commons Special Committee on the Review of the *CSIS Act* and *Security Offences Act*, discussed below. Neither in its public hearings nor in its private meetings was there discord. On only one issue was a vote taken. Several reasons might explain such relations. Perhaps most important, the committee was established

by statute with a specific mandate and time frame. Thus, committee members took their responsibilities very seriously, missing few meetings. Significantly, the committee had a very experienced chair, who had previously chaired both a standing committee and special statutory reviews. The committee also had more staff than most parliamentary committees.[36]

Left out of the Senate special committee's equation was the potential negative impact of not having Parliament directly involved in the process of political accountability. During the passage of the legislation, the government had positioned SIRC as a "surrogate for Parliament." Such a claim was, at best, only partly true. To be sure, having a quasi-independent body to conduct reviews of CSIS would be helpful insofar as it could comment on the propriety (and to a lesser extent the efficacy) of the organization, and its reports, once eventually tabled in Parliament by the responsible minister, would provide an accounting of the agency. However, the fact that Parliament would neither have access to the matters underpinning the reports nor be able to receive detailed answers from SIRC effectively diminished its capacity to hold the government ministers properly to account, especially regarding important political questions.[37] Thus, SIRC has not been, and cannot be, a true surrogate for Parliament where accountability is concerned. Both independent review and the capacity to call the responsible minister to account are necessary. As Franks argued in 1980:

> Parliament's ability to serve as a useful watchdog over security matters depends, as in other matters, on the effectiveness of the flow of information. The secrecy involved in matters of state greatly restricts this flow. Faced with a claim by government that information must remain secret because it is "not in the public interest (or national interest)" to reveal it (i.e. for reasons of state), Parliament has few tools, apart from persistent nagging, to cast doubt on the claim. Parliament cannot, for example, question civil servants to discover whether ministers are telling the truth, or are concealing information. Nor can Parliament or its committees obtain copies of reports or papers which a minister refuses to release. As long as it is in order, any answer, or none at all, is an acceptable ministerial response to a question, both on the floor of the House and in committee. With all these obstacles, it is difficult for Parliament to distinguish between a justified secrecy for worthwhile reasons of state or less justifiable secrecy to avoid embarrassment to the government or bureaucracy, that is, for reasons of office. (20-1)

Implementing McDonald: the *CSIS Act* and the *Security Offences Act*

The immediate reaction of the government to McDonald's recommendations was not encouraging. An official riposte was prepared challenging a number of points in the report. In the longer run, however, McDonald did have a decisive impact on national security accountability, although not always directly. We have already described the role of the Pitfield Committee in amending the legislation that was passed into law in 1984 as the *Canadian Security Intelligence Service Act*, creating the new civilian security intelligence agency, CSIS. The new agency was to be made accountable in numerous ways that its RCMP predecessor was not, but the new procedures did not always follow McDonald's guidelines. In the passage from McDonald to the *CSIS Act*, some changes were added and new byways taken; some recommendations disappeared completely (Farson 1991b, 157-88).

The most central element in the accountability framework for CSIS lay in the legislation itself. Unlike its predecessor, CSIS has a statutory mandate. The McDonald Commission had been highly critical of the absence of a legislative mandate for the RCMP Security Service. Following the commission's report, the *CSIS Act* itself was to be the bedrock of accountability for the new agency, spelling out in statutory form the agency's fundamental mandate, its powers and the limits on its powers, as well as the institutional framework in which it was to operate and report. CSIS is empowered to collect, analyze and retain information and intelligence "respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada" and provide threat assessments to the federal government or, by approved arrangement, to the provinces, foreign governments or international organizations (sections 12 and 13). Threats to the security of Canada are defined in section 2:

> (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
>
> (b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,
>
> (c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state,[38] and

(d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).

CSIS is thus provided with a descriptive list of activities it may legitimately target, and those it may not. Espionage, sabotage, terrorism and other forms of political violence and clandestine foreign-influenced activities detrimental to Canadian interests are all relatively noncontroversial as threats to security. The inclusion of activities described in 2(d) – in effect, the controversial concept of "subversive" activities – has led to demands that this definition be removed or modified, especially after 1987, when the solicitor general, following recommendations made initially by SIRC and subsequently by the Independent Advisory Committee, directed that the Counter-Subversion Branch of CSIS be disbanded, with retained files distributed to more appropriate operational branches or dispersed to the archives (SIRC 1989, 1). The line between activities described in 2(d) and "lawful advocacy, protest or dissent" might not always be easy to draw in practice. It is clear, however, that the definitions of legitimate and illegitimate targets have had important consequences for the accountability of CSIS, providing a legal baseline for judging the appropriateness of the agency's targeting. Drawing on the defined threats in the *CSIS Act*, the agency has for some years indicated that it does not target threats to national unity, such as the lawful forms of the Quebec sovereignty movement, unless it has reason to believe they are being carried out in conjunction with activities described in sections 2(a) to (d).

With regard to internal controls, the ministerial and administrative lines of responsibility suggested by McDonald were largely followed. Significantly, the head of the service was expressly made responsible for its control and management under the "direction of the Minister." However, two steps were taken to make the minister and the incumbent's deputy more aware of the service's activities. One was an obligation on the part of the director to consult broadly with the deputy minister. This included any matter designated by ministerial directive for consultation, as well as all operational policies and warrant applications (sections 6 and 7). The other, following US practice, concerned the establishment of an additional set of "eyes and ears on the Service" through the office of the inspector general (IG) of CSIS.

Judicial controls over intrusive surveillance methods (except for human sources) were adopted in the Act, with rules imposed on CSIS for making applications to the Federal Court for warrants for interception of communications.

In terms of external review, financial audits by the auditor general were not enshrined in legislation, although this idea was followed up in practice more than a decade later. The two proposed independent external review bodies were merged into one body, the Security Intelligence Review Committee, an institution exhibiting some significant differences from the models proposed by McDonald.[39]

The most significant divergence from McDonald was the decision not to follow up on the recommendation regarding a joint parliamentary committee to examine security and intelligence issues in camera. Instead, as Solicitor General Robert Kaplan said several times during the debates over the *CSIS Act* in the House of Commons, SIRC was supposed to be a "surrogate for Parliament." There was, however, a statutory provision for a five-year parliamentary review of the Act, as well as an indication that the mandated annual report of SIRC should be tabled in both houses of Parliament after being examined first by the minister. Apart from these two exceptions, the legislation remains silent on the role of Parliament.

Law enforcement versus security intelligence

A crucial feature of the *CSIS Act* is that all of the accountability elements are uniquely institution-specific. That is to say, not all the various national security functions of the Canadian government are provided with systems of accountability, only those exercised by CSIS. But CSIS was not, and is not, the only department or agency of government involved in national security activities. We believe that institution-specific review bodies represent a potentially crucial weakness where there is an overlap in function, as they would have to rely on the good nature of other parties, not the law, to scrutinize such practices in detail.

The *CSIS Act* was passed in tandem with the *Security Offences Act*. The latter legislation authorizes the attorney general of Canada to conduct proceedings in respect to any criminal offence arising out of conduct constituting a threat to the security of Canada within the meaning of the *CSIS Act*. The RCMP is designated as the criminal law enforcement agency

responsible for investigating such offences. Despite the creation of CSIS as a civilian security intelligence agency, the RCMP thus never vacated the field of criminal law enforcement with regard to national security offences. This assignment of roles was of course necessary since CSIS was deliberately not given any law enforcement powers. However, no accountability was assigned to the RCMP with regard to its national security activities under either the *CSIS Act* or the *Security Offences Act*. In 1985, revisions to the *Royal Canadian Mounted Police Act* called for a public complaints process, which was established in 1988.[40] The Commission for Public Complaints against the RCMP (known as the CPC) was constituted to investigate citizen complaints about RCMP criminal law enforcement, not national security activities. As later indicated by the Maher Arar inquiry and the testimony of two successive CPC chairs (see below), the CPC has proved inadequate in providing accountability in this area.

The Pitfield Committee had laid particular stress on the differences between security intelligence and law enforcement, and on the "severe consequences on a person's life" that security investigations could have: "Thus the question of control and accountability becomes important, because there is no impartial adjudication by a third party of the appropriateness of an investigation. Since it is so open-ended and confidential in nature, security intelligence work requires a close and thorough system of control, direction and review, in which political responsibility plays a large part. Such close direction is at odds with traditional Canadian notions of law enforcement" (Senate Special Committee on the Canadian Security Intelligence Service 1983, 6).

The key to understanding accountability in the *CSIS Act* lies in the separation of the security service from the RCMP with its law enforcement role. Parliament, the Senate committee and the McDonald Commission before them all proceeded on the basis that accountability, both as control and as review (explanation), was incompatible with the principle of police independence and with an arm's-length relationship between the executive and law enforcement.

Directly related to this issue of police independence was one of the most significant problems identified by the McDonald Commission: the lack of clear ministerial responsibility for the activities of the RCMP Security Service. Ministers of the Crown had indicated repeatedly that the principle of police independence compelled them to remain in ignorance of security service operations. The best-known iteration of this argument came from Prime Minister Pierre Trudeau in 1977:

> I have attempted to make it quite clear that the policy of this government, and I believe the previous governments in this country, has been that they...should be kept in ignorance of the day to day operations of the police force and even of the security force. I repeat that this is not a view that is held by all democracies but it is our view and it is one we stand by. Therefore in this particular case it is not a matter of pleading ignorance as an excuse. It is a matter of stating as a principle that the particular minister of the day should not have a right to know what the police are doing constantly in their investigative practices, what they are looking at, and what they are looking for, and the way in which they are doing it...That is our position. It is not one of pleading ignorance to defend the government. It is one of keeping the government's nose out of the operations of the police at whatever level of government. (Edwards 1980, 94)

Trudeau's position was quite unsatisfactory with regard to accountability for national security, whatever the validity of the rationale for police independence for criminal law enforcement. The *CSIS Act* responded to this concern in part by assigning statutory responsibility for CSIS to the solicitor general (now the minister of public safety).[41]

Ministerial control: the inspector general

Ministerial oversight of CSIS is further strengthened by the office of the inspector general. The IG was not part of the McDonald Commission's recommendations. The IG is appointed by the governor-in-council and is responsible to the deputy minister of public safety. The IG monitors compliance by CSIS with its operational policies, reviews operational activities and is to have unimpeded access to any information under the control of CSIS that the IG deems necessary for the discharge of his or her responsibilities. The IG submits certificates to the minister pursuant to periodic reports on the operational activities of CSIS prepared by the director for the minister. The *CSIS Act* states that these certificates attest to the extent to which the IG "is satisfied with the director's report" and to whether, in his or her opinion, CSIS activities are in compliance with the Act and with ministerial directives. The certificates also state the IG's opinion as to whether there was any "unreasonable or unnecessary exercise by the Service of any of its powers" (sections 30-33). Although these reports and certificates are transmitted to SIRC, there is no provision for their tabling in Parliament or any form of

publication, although most have subsequently been declassified in redacted form in response to access-to-information requests.[42]

The office of the IG is conceived strictly as contributing to executive control by enhancing ministerial responsibility. It does this by serving as an independent set of internal "eyes and ears" on the activities of CSIS for the minister and by providing assurance. While this assurance plays a crucial role in ensuring compliance, it also covers certain matters of efficacy, particularly by identifying gaps in CSIS's legislative and policy framework. Because the IG operates within the machinery of government, finding the right balance between cooperation, on the one hand, and independence, on the other, is not always easy. The IG may also be tasked by SIRC to conduct a review of specific activities of CSIS.[43]

The history of relations between the IG, CSIS and the minister has been mixed, with strains sometimes clearly evident.[44] Although the IG is supposed to have access to all relevant documentation, "cabinet confidences" may be withheld. This could be a significant limitation, as the government treats cabinet communications to CSIS, crucially including ministerial directives, as falling into this category. However, a number of ministerial directives and guidelines to CSIS have been made public, in whole or in part, via releases under the *Access to Information Act* and SIRC reports. Those dealing with the handling of human sources – not covered by judicial controls over technical surveillance – and the targeting of so-called "sensitive" institutions, such as universities and religious organizations, suggest that fairly strict guidelines are imposed on CSIS actions.[45]

Judicial oversight and internal control

Sections 21 to 28 of the *CSIS Act* specify the conditions by which the service may apply for judicial warrants that authorize the interception of communications, the installation of surreptitious surveillance devices, the entering of private premises and the search and seizure of documents, records, information or any other thing. Such applications must be made in writing and accompanied by an affidavit of fact indicating reasonable grounds for believing that the target may constitute a threat to security as defined in the Act, and that other, less intrusive methods of investigation are likely to prove inadequate. The target, including the person or persons, the place and the information or things sought, must be specified. Warrants are also limited in duration, no more than one year, although application may be made for renewal. Warrant applications are heard only by specially designated judges of the Federal Court. Such hearings are held in a secure courtroom and in camera. To expedite the process, at least one designated judge is on duty at all times to hear applications. In contrast to Criminal Code wiretaps, there is no subsequent obligation to reveal that a target has been the subject of an intrusive investigation.

Early in CSIS's institutional history, in 1987, a warrant application containing incorrect information led to the resignation of the first CSIS director and to the compromising of a case against conspirators planning to assassinate a visiting minister of a foreign government (Cleroux 1990, 184-9).[46] Following that, and in part in response to earlier suggestions from SIRC on strengthening the warrant application process, CSIS has constructed elaborate, multi-step internal control mechanisms for approval of applications.[47] This has led one observer to suggest that the main impact of the judicial control of surveillance applications may actually lie in the internalization of the control process within CSIS (Leigh 1996, 173). Very few warrants are now rejected. This may well be due to the fact that the prior internal process, including ministerial approval and scrutiny by Department of Justice lawyers, weeds out poor warrant applications before they are submitted to the court.

It should be noted that the role of judicial oversight in national security is by no means limited to the control mechanism of warrant approval under the *CSIS Act*. The judiciary also plays an important role in interpreting national security statutes, ruling on the constitutionality of legislative provisions, assessing the fairness of hearing procedures and considering the reasonableness of security certificates under the *Immigration and Refugee Protection Act*[48] and the appropriateness of applications regarding the public disclosure of evidence under the *Canada Evidence Act*. Judges have also played a crucial role as commissioners of public inquiries into national security activities, and one review office, the commissioner of the Communications Security Establishment Canada, according to statute, must be headed by a supernumerary or retired justice.

External review: the Security Intelligence Review Committee

SIRC is constituted as a committee consisting of a chair and between two and four other members.[49] All members of the committee must be privy councillors not serving in

Parliament.[50] They are chosen by the prime minister after "consultation" with the leader of the opposition and the leaders of each recognized party in the House of Commons. The implication of this consultation, never actually spelled out, is that the membership of SIRC broadly reflects the partisan makeup of the House, thus supposedly substituting for the representative role of the parliamentary committee unsuccessfully recommended by the McDonald Commission. There has never been any formal recognition of this putative principle. Furthermore, any semblance of mirror representation of Parliament has not been the practice since the Bloc Québécois became the official opposition in the 1993 election, as its members have refused to take the privy councillor's oath and to swear allegiance to the Queen of Canada.[51]

As sworn privy councillors, the members of SIRC are in effect considered to meet the same security requirements applicable to CSIS officers; according to the *CSIS Act*, SIRC employees must be vetted and take an oath of secrecy (section 37). SIRC, which adheres to the government security policy and thus works in a secure environment, is entitled to have full access to all information it requires from CSIS and the IG, save cabinet confidences (section 39).[52]

SIRC is mandated to "review generally" the performance by CSIS of its duties and functions, including reviewing the reports of the CSIS director and the certificates of the IG; reviewing directions issued by the minister to CSIS; reviewing any arrangements made by CSIS with provincial governments, departments or agencies and police forces; monitoring intelligence sharing that stems from such arrangements; reviewing CSIS arrangements with foreign governments, departments and agencies and with international organizations and monitoring international intelligence; reviewing reports of unlawful behaviour by CSIS employees; monitoring requests made by the minister of national defence or the minister of foreign affairs for assistance in the collection of foreign intelligence within Canada; reviewing regulations under the Act; and compiling and analyzing statistics on CSIS operational activities (section 38). Since its inception in 1984, SIRC has prepared some 178 review reports, of which about 40 have resulted from a request by the minister under section 54 of the *CSIS Act*. Most of these reports have been released in redacted form under the *Access to Information Act*. It should be noted, however, that the practice of ministers requesting such reports has declined since the early years of CSIS, with less than 25 percent of all requests having been made since 1996.

SIRC submits annual reports to the minister, who in turn tables them in Parliament. These reports may be redacted by the minister to protect national security and personal privacy. The annual reports, available on the SIRC website, cover both the committee's review and complaint investigation functions. Section 40 of the *CSIS Act* authorizes SIRC to conduct reviews, or to direct CSIS or the IG to conduct reviews, to ensure that the activities of the service are carried out in accordance with the Act, regulations and ministerial directions, and that the activities "do not involve any unreasonable or unnecessary exercise by the Service of any of its powers." SIRC may thus task the IG to review particular matters, or "where it considers that a review by the Service or the Inspector General would be inappropriate, conduct such a review itself." In addition, section 54 of the *CSIS Act* provides that SIRC may, on request by the minister or at any other time, furnish the minister with a special report concerning any matter that relates to the performance of its duties and functions. From 1984 through 2006, SIRC has made 39 section 54 reports. These may include inquiries into particular allegations, or they may be more systemic in nature. Reference to them is normally made in the annual reports.[53] However, by the time such reports are tabled, the events covered have sometimes occurred as much as 18 months previously and have lost their news value and capacity to gain Parliament's attention.

SIRC develops an annual research plan on a selective basis since it lacks the resources to review all potentially relevant matters. Each annual report typically includes a regional office review and an audit of a security liaison officer (SLO) post abroad, with further topics selected for in-depth inquiries. In selecting topics, SIRC looks to factors such as the international threat environment, issues arising from complaints, government policy changes with implications for CSIS operations, SIRC's public undertakings to look into particular matters and SIRC's statutory obligations. In conducting these in-depth inquiries, SIRC typically reviews all relevant CSIS documents and files, electronic and in hard copy. These include targeting authorizations, warrants with supporting documentation, operational reports, human source logs, internal CSIS correspondence and records of exchanges of information with other agencies and departments including, where relevant, international agencies. SIRC may also conduct interviews and field investigations. CSIS makes a separate office with

computers available at CSIS headquarters in Ottawa for the exclusive use of SIRC staff. Parliament, it should be noted, has no ongoing way of knowing how thorough these reviews are or whether they use acceptable research practices.

Targeting review

Within CSIS, the Target Approval Review Committee (TARC) is the senior operational committee charged with considering and approving applications by CSIS officers to launch investigations.[54] SIRC reviews targeting authorizations made by TARC to ensure compliance with the *CSIS Act*, ministerial directions and relevant operational policies. SIRC examines whether CSIS had reasonable grounds to suspect a threat to the security of Canada in seeking its targeting approval, whether the level and intrusiveness of the investigation were proportionate to the seriousness and imminence of the threat, whether the service collected only that information strictly necessary to advise the government of a threat, whether CSIS respected the rights and civil liberties of individuals and groups, and whether any information was exchanged with other agencies (SIRC 2003, 14-16). On occasion, SIRC has indicated concerns about aspects of targeting and conveyed advice to CSIS on changes in procedure.

Foreign intelligence

Under section 16 of the *CSIS Act*, the minister of foreign affairs or the minister of national defence may ask CSIS to collect intelligence in Canada concerning the "capabilities, intentions or activities" of a foreign state. SIRC annually reviews all ministerial requests for section 16 operations to ensure compliance with the Act, as well as compliance with a memorandum of understanding to the effect that any request must contain an explicit prohibition against targeting Canadians, permanent residents and Canadian corporations, and that the request should indicate whether the proposed activity is likely to involve Canadians (SIRC 1998, 53). SIRC reviews section 16 operations on a randomly selected audit basis and has identified errors. CSIS requests to the Communications Security Establishment Canada (CSEC) for access to that agency's communication intercepts are routinely scrutinized by SIRC to ensure that they comply with existing law and policy.

Former CSIS director Ward Elcock has publicly stated on several occasions that his interpretation of section 12 of the *CSIS Act* permitted CSIS to collect intelligence abroad as well as in Canada, so long as the intelligence was related to threats to the security of Canada as specified in the Act. On this basis, CSIS has acknowledged its growing role as an intelligence collector outside Canada since 9/11. While this is not precisely a foreign intelligence role similar to that performed by the US Central Intelligence Agency or Britain's Secret Intelligence Service, in that political, economic or military intelligence that does not relate to threats to Canadian security or Canadian interests would fall outside the CSIS ambit, this expanded international role is one that challenges existing accountability procedures in terms of both propriety and efficacy. The current IG, for example, has suggested that CSIS lacks a suitable framework for its operations in Afghanistan. The Federal Court's rejection of a CSIS warrant application that would have permitted its personnel to follow suspected Canadian citizens to unidentified countries and then to intercept their communications, on grounds that the court had no authority to endorse such a warrant, further exemplifies shortcomings in the law and oversight procedures (Freeze 2008).

The Afghan theatre is also the locus of operations for other national security organizations. John Adams, the current chief of the CSEC, has publicly acknowledged that his agency is operating there. To these must be added the operations of the military's new HUMINT (human intelligence) unit and the much expanded JTF2 (Joint Task Force 2), the rules of engagement of which are not known (Akkad 2008).[55] Although all military personnel are subject to the Code of Service Discipline, the only unit within Canada's military that is subject to independent oversight would appear to be its military police. During the 1990s, two special advisory groups, headed by former chief justice Brian Dickson, had recommended improving the military justice system. The report of the Létourneau Commission into the torture and killing of a Somali teenager was more damning, pointing to a failure of leadership and a lack of accountability in the Canadian Armed Forces and a failure of Parliament to scrutinize them adequately or to engage in policy development (Commission of Inquiry into the Deployment of Canadian Forces to Somalia 1997). The government responded by disbanding Canada's elite Airborne Regiment and by establishing the Military Police Complaints Commission in December 1999. This is a quasi-judicial, independent civilian agency that now examines complaints about the conduct of members of the military police in performing their policing activities or about interference

in or obstruction of their investigations. Since 9/11, there has been no clear evidence that any of Canada's national security agencies have been involved in either torture[56] or extraordinary rendition, matters that have tarnished their American counterparts and that have largely escaped oversight in the US. Recently, concern has been expressed about the treatment Canadian-captured Taliban fighters have received after being handed over to Afghan authorities ("New Case of Afghan Prisoner Abuse" 2007).

Foreign intelligence sharing

SIRC reviews written arrangements for cooperation with foreign intelligence services, to ensure compliance with the *CSIS Act* and with ministerial directives and conditions for approval. SIRC has also examined the human rights record of host countries, and has flagged relationships where CSIS should be vigilant in ensuring that no intelligence transferred to a foreign agency results in human rights abuses. SIRC also examines the substance of information exchanged under any given foreign arrangement during the course of its regular reviews of SLO posts abroad.

Warrants

SIRC annually reviews the use of Federal Court warrants by CSIS. In its 2001-02 annual report, SIRC stated:

> Warrants are one of the most powerful and intrusive tools in the hands of any department or agency of the Government of Canada. For this reason alone, their use bears continued scrutiny, which task the Committee takes very seriously. In addition, our review of the Service's handling of warrants provides insights into the entire breadth of its investigative activities and is an important indicator of the Service's view of its priorities.

SIRC's examination of the warrant process covers such matters as warrant acquisition, warrant implementation and applicable court decisions and regulations. In addition, it produces warrant statistics. In reviewing the obtaining of a warrant, SIRC examines all documents relating to how the warrant applications were prepared, including the affidavits and supporting documentation, working files relating to the affidavit, the requests for targeting authority and the TARC minutes. In reviewing this documentation, SIRC seeks to ascertain whether the affidavits are factually correct and adequately supported in the documentation and include all pertinent information, and whether the affidavits are complete and balanced, with the facts and circumstances of the cases fully, fairly and objectively expressed (SIRC 2002, 21).

Complaints

SIRC has a mandate to investigate two categories of complaints pursuant to sections 41 and 42 of the *CSIS Act*: complaints made with respect to "any act or thing done by the Service" and complaints relating to the denial of security clearances for federal government employees or prospective employees, as well as for federal government contractors. SIRC also has a mandate to conduct investigations in relation to denials of citizenship applications on security or criminal grounds by the minister of immigration.[57]

From its inception to March 2005, SIRC received 883 complaints and produced 118 written reports following investigations of complaints, involving either written or oral hearings (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar 2006b, 174-5).[58] In hearings, special procedures are designed to balance procedural fairness with national security concerns.[59] According to the *CSIS Act*, when investigating a complaint concerning the denial of security clearance, SIRC sends a statement to the complainant summarizing such information available to SIRC "as will enable the complainant to be as fully informed as possible of the circumstances giving rise to the denial of the security clearance" (section 46). Investigations of complaints are conducted in camera. SIRC has the power to summon witnesses, to compel documents to be produced and to administer oaths. The complainant, CSIS and relevant departments are all given the right to make representations to SIRC, to present evidence and to be represented by counsel. The Act provides, however, that "no one is entitled as of right to be present during, to have access to, or to comment on representations made...by any other person" (sections 50 and 48[2]). SIRC's Rules of Procedure provide for discretionary disclosure of evidence and representations to parties, subject to section 37 of the Act, but state that it is within the discretion of the member conducting the investigation, in "balancing the requirements of preventing threats to the security of Canada and providing fairness to the person affected," to disclose the representations of the parties to one another (SIRC 2005). In the case of an *ex parte* hearing (where parties are excluded), SIRC counsel will cross-examine witnesses. As one commentator notes: "Since committee counsel has the requisite security clearance and has had the opportunity to review files not available to the complainant's counsel, he or she is also able to explore issues and particulars that would be unknown to the complainant's counsel" (Rankin

1990). When a party is excluded from a hearing for reasons of national security, he or she may be provided with the substance of the evidence given or representations made, although this is discretionary. The Supreme Court of Canada[60] has held that the rules recognize and strike a fair balance between the competing interests of the individual in fair procedures, and the state's interest in effectively conducting national security and criminal intelligence investigations and in protecting police sources (Arar Commission 2006a, 275-6).

SIRC is limited in its powers to making findings and recommendations. In this regard, the Supreme Court has held that its recommendations are not binding on the government.[61]

The McDonald Commission had recommended the creation of a separate Security Appeals Tribunal, presided over by a Federal Court judge, to hear appeals relating to immigration, citizenship and security clearances (Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police 1981, 1:421-6, 2:805-11). McDonald saw this tribunal as a quasi-judicial body. "Given the adversarial nature of proceedings before the tribunal, and the need for the tribunal to function as much as possible like a Court, we think it should be quite separate from the Advisory Council on Security and Intelligence which will have a broad mandate to review and advise the government on all aspects of security and intelligence policy and operations" (2:883). In the *CSIS Act*, however, review and complaints are combined in the same body. Combining the two functions in one body does offer certain advantages from the point of view of accountability. SIRC insists that it gains a more comprehensive understanding of CSIS operations than would be possible if it were limited to review alone (Leigh 1996, 160).

SIRC and CSIS: evolution of the review process

Since 1984, the relationship between SIRC and CSIS and the nature of the accountability process have evolved with experience. The context within which both the agency and its review body operate has undergone some dramatic changes.

The first half decade following the *CSIS Act* fell within the continuing context of the Cold War. The continuing assumption was that the main security threat to Canada came from the Communist bloc. Counter-espionage was a leading priority for CSIS. Counter-subversion – a priority throughout the earlier Cold War period – was increasingly being questioned, a process to which SIRC contributed through its critical reviews of the service's operations, leading in 1987 to the closing of the Counter-Subversion Branch of CSIS on ministerial order.[62]

Counterterrorism became a leading concern as well, especially after the Air India bombing in 1985 took the lives of 329 people, the vast majority of them Canadians. The failure to prevent that attack, the shortcomings of the investigation (criminal proceedings began only in 2003 and have yet to result in any convictions for direct responsibility) and evidence of lack of cooperation between CSIS and the RCMP all contributed to increased demands for greater accountability. In 2005-06, two special investigations of the Air India affair were called; the second was a full-scale judicial inquiry under a retired Supreme Court justice,[63] indicating a serious lack of satisfaction with the level of accountability produced by the SIRC/CSIS process two decades earlier.

The decade of the 1990s was a transition to a post-Cold War era. With the collapse of the Communist bloc and the dissolution of the Soviet Union, the old Cold War paradigm disappeared; but in this decade there was no clear successor paradigm to replace the old one. Government economy measures were being extended to encompass security and intelligence as well as other functions, and CSIS found its budget under constraint at the same time as it had to redefine its role in a changing threat environment. In 1994, SIRC was called upon to undertake a major public accounting of a scandal that beset CSIS. The "Heritage Front affair" involved the naming in the media of a CSIS source within an extreme right-wing organization and a series of questions that arose from this revelation. The report of a section 54 special investigation was made public, with a few parts removed on security grounds (SIRC 1994).

The third period was dramatically initiated by the terrorist attacks of September 11, 2001, on New York and Washington, DC, and the declaration by the US government of a "war on terrorism" in which Canada has become a participant. New powers to combat terrorism were passed by Parliament and new resources invested. CSIS has stepped up its security intelligence collection capacity abroad (Freeze 2006). Other agencies, including the RCMP and the CSEC, have become more active in anti-terrorist activities. Domestically, a new umbrella department of government, Public Safety Canada, has been created to direct the security and intelligence functions of government. And the first official National Security Policy has been published (Farson and Whitaker 2008).

Since 9/11, there has been one serious scandal associated with the conduct of security intelligence, the Maher Arar affair, that brought in its wake a major commission of inquiry that has made important recommendations for overhauling the entire regime of accountability with regard to national security activities (see below for more about these policy recommendations, to which the government has not yet responded). Though the commission of inquiry was ostensibly charged with establishing an enhanced review system for the RCMP, it also recommended bringing several agencies not hitherto formally scrutinized under an independent external review body. Two other public inquiries were also established. One, the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, under Frank Iacobucci, was similar in nature to the Arar Commission but conducted its proceedings in private and its terms of reference did not require policy recommendations. The other, the commission of inquiry into the Air India bombing under John Major, has yet to report and may well have recommendations with serious implications for accountability in the future.

Institutionally, SIRC has moved over the two and a half decades of its existence from an early period of relatively aggressive behaviour in establishing itself in relation to CSIS and defining its role (under the leadership of SIRC's first chair, Ronald Atkey, from 1984 to 1989), to a period of contraction and flux in the early 1990s, to a period in which the review committee seems to have settled into a relatively stable institutionalized relationship with its subject agency. CSIS today speaks publicly in generally supportive terms of its review body, while SIRC underlines the good working relationship that it has established with CSIS. While this may seem to signal a positive interpretation of effective accountability, some critics argue that too cozy a relationship suggests a review body "captured" by the agency it is supposed to scrutinize but on which it is dependent for its information.[64] There is perhaps a certain inevitability over the long term for reviewer and reviewed to grow more comfortable with each other, just as the history of regulation suggests a tendency for the regulator and the regulated to become ever more accommodative of each other. There are definite dangers in this, but SIRC has not lost its capacity to focus public attention on CSIS shortcomings, as it has continued to do in recent years.[65]

There is a public perception problem: SIRC's effectiveness is difficult to assess given the degree to which most of its review activities are necessarily shrouded in secrecy, or semi-secrecy. Stripped of nondisclosable information, its annual reports provide only limited public enlightenment and rarely attract much media attention. Occasional special section 54 reports may cover topics of public concern, but are usually entirely or mostly classified, with only occasional glimpses coming to light via access-to-information requests. Some observers have suggested that SIRC's main impact may be found in the internal procedures and "culture" of CSIS, reflecting an internalization of some of the norms of accountability that SIRC has advanced, and in the ability of CSIS to avoid pitfalls and usually stay out of trouble, partly as a result of external review of its operations (Gill 1989).[66]

The five-year review of the *CSIS Act* and *Security Offences Act*

The only parliamentary function that the *CSIS Act* and *Security Offences Act* envisaged was the establishment of a special committee in 1989 to review the two acts after they had been in operation for five years.[67] For this purpose, Parliament was given one year to complete its task. Though this committee was required by statute to conduct a "comprehensive review of the provisions and operation [of the two Acts]," the special committee soon found itself facing numerous roadblocks that ultimately prevented it from fulfilling its legal obligations within the time available. Significantly, it found it impossible to obtain access to particular people, papers and records.[68] Furthermore, its "surrogate" would not speak freely about what underpinned its various reports and what its recommendations to the minister had been. Despite these difficulties, it was able to determine that at least one of SIRC's reports was seriously flawed methodologically, a point on which SIRC subsequently concurred (Farson 1995, 185–212). Because it was denied access to key records and was unable to determine whether the flawed SIRC report was typical or atypical, Parliament was unable to determine whether the various requirements of the legislation were being met, particularly those aspects concerning accountability, control and review.

Most of the special committee's recommendations were dismissed without explanation.[69] In three areas, however, it had modest success. The first concerned the decision by the government to require the director of CSIS to provide a public version of the CSIS annual

report. Second, and perhaps not surprisingly, the special committee recommended the establishment of a parliamentary committee that would have broad and guaranteed access to the secret world and its review bodies. Though the government ignored this recommendation, as it had a similar one by McDonald, Parliament took up its fallback position and established the Subcommittee on National Security of what was then the Standing Committee on Justice and the Solicitor General. The idea was to produce the least threatening type of committee to look at a broad range of national security issues.[70] Variations of this committee have been established in subsequent Parliaments. Few have taken up the items that the special committee thought should form part of its workplan. Their impact on the policies and procedures of the broader intelligence remit have remained limited, sometimes even failing to consider the annual reports of SIRC and the director of CSIS. In part, this was due to the broadening of party representation in the House of Commons in the 1990s from three to five. Significantly, one of these new entities was the Bloc Québécois, a party that wanted independence from Canada for Quebec. Given that it at one point became the official opposition, this raised difficult questions if Parliament was to be deeply engaged in overseeing Canada's security and intelligence community. In its most recent incarnation, the national security subcommittee has tended to morph into a subcommittee of the whole Justice committee that has not confined itself to national security matters.

Perhaps the special committee's most important impact concerned something not found among its recommendations. Staff of the special committee were authorized in 1990 to strike an agreement with the Office of the Auditor General for the latter to consider the work of Canada's security and intelligence community. Though work did not begin until 1996, largely because of the amount of discussion needed to reach an agreement with the government on what would be considered and how security procedures would be maintained, the OAG has since become an important player in the review of the efficacy of Canada's security and intelligence community, focusing its attention on at least one organization or a particular practice in each of its recent annual reports.

The office of the CSE commissioner

Another idea that did eventually come to fruition concerned the establishment of a form of review for arguably Canada's most secret intelligence agency, the Communications Security Establishment Canada (Rosen 1993). As Canada's primary electronic eavesdropping agency, the CSEC (called the Communications Security Establishment, or CSE, until September 2007) collects foreign intelligence through technical rather than human sources. It intercepts, decrypts, retains and analyzes foreign communications in support of Canadian defence and foreign policy, and offers protection services for electronic information and communication within the government of Canada. It also provides technical and operational assistance to federal law enforcement and security agencies under their respective warrant processes.

The CSEC began during the Second World War and continued into peacetime as the Communications Branch, National Research Council (CBNRC). After its existence was exposed by the media in 1975, the CBNRC was transferred to the Department of National Defence and renamed the Communications Security Establishment through a series of rather innocuous orders-in-council.[71] From its origins, the agency's budget was deliberately hidden, and indeed its very existence was an official but poorly kept secret until 1983, when public acknowledgement was made by the government during the debate on the *CSIS Act* (Senate Special Committee on the Canadian Security Intelligence Service 1983, 18-19, 23, 31-3).[72]

In 1990, the special committee that conducted Parliament's five-year review of the *CSIS Act* recommended that the CSE be given a statutory basis as well as a review mechanism (House of Commons Special Committee on the Review of the *Canadian Security Intelligence Act* and the *Security Offences Act* 1990, 153). The privacy commissioner and the auditor general[73] subsequently reiterated these concerns about the lack of a statutory mandate.

The review system was achieved in an unusual way when Derek Lee, a former member of the five-year review committee and then the chair of the Subcommittee on National Security, placed a motion on the order paper. Amid public criticism of the lack of transparency in CSE operations and media allegations of wrongdoing, the government eventually acted but not through Parliament. Though the special committee had recommended extending SIRC's mandate to include the CSE, it chose instead to create a new office: commissioner of the CSE. The government's method was through an order-in-council, which again avoided any discussion in Parliament of the mandate of either the CSE or the commissioner until the debate over the *Anti-*

terrorism Act in 2001. Significantly, this gave the commissioner of the CSE all the powers provided under part II of the *Inquiries Act*. Thus, unlike SIRC and the IG, which have the right of access to information and personnel, the commissioner has subpoena powers. These provide the incumbent with guaranteed and immediate access to both personnel and records of the agency, and the authority to require persons to give evidence under oath. The CSE commissioner's mandate was originally "to review the activities of the [CSE] to determine whether those activities are in compliance with the law,"[74] including the Criminal Code, the Charter of Rights and Freedoms, the *Privacy Act* or any other relevant legislation (and, most important, since 2001, the mandate itself). An annual report must be submitted to the minister of national defence with an unclassified version to be tabled in Parliament. The commissioner may also submit classified reports to the minister when the commissioner considers it advisable.[75] Crucially, the order-in-council did not provide a statutory mandate for the agency, a serious omission regularly underlined by the CSE commissioner himself in his annual reports.[76] In 1999, the commissioner's mandate was extended to encompass a complaints function. Thus, citizens may file complaints about the lawfulness of CSEC activities with the Office of the Commissioner. A Complaints Review Committee then recommends whether further investigation is required. The commissioner must inform a complainant of the results of an investigation, while not disclosing any classified information.

In 2001, the commissioner's mandate was finally formalized under the *Anti-terrorism Act* and expanded to authorize the interception of private communications of Canadians under certain specified conditions.[77] The commissioner is now directed to review activities carried out under such ministerial authorizations to ensure that they are in compliance with the conditions of the authorization, and to report any findings in the annual reports. In this regard, it is important to note that both the current commissioner and his predecessors believe that the current legislation "lacks clarity and ought to be amended."[78] Any CSEC activity that the commissioner discovers that does not comply with the law must be reported to the minister and the attorney general.

In our view, the commissioner's mandate is insufficient in that it deals only with certain aspects of propriety. While there is a requirement to certify that the agency has complied with law, regulations and policy, there is no specific forward-looking obligation to establish whether these remain either appropriate or adequate, particularly in light of a continuously changing threat environment and rapid advances in communications technology. Significantly, there is no mandate to establish whether the CSEC operates efficaciously.[79]

When the government sought to rush through its omnibus anti-terrorism legislation immediately after 9/11, Parliament was forced to focus its attention on the most immediately worrisome parts of the legislation. Consequently, it had little opportunity to consider the role of the CSEC, what the mandate of the commissioner should be or how that office might report to Parliament. A comparison between this study's handling of the CSEC's mandate and that of CSIS when the *CSIS Act* was adopted in 1983-84 (particularly regarding such matters as the duration of the study; the number, type and region of the country of witnesses heard; and the briefs considered) is instructive. Despite the fact that the CSEC is arguably just as secretive and as potentially intrusive into individual privacy as CSIS, the CSEC experience pales by comparison. Other important attributes of the legislation were also given short shrift.

The impact of the CSE commissioner's work has been mixed. On the positive side are the numerous recommendations accepted by government. Writing in his 2005-06 annual report, the commissioner stated:

> Of almost 100 recommendations made by the CSE Commissioner, 75 percent were accepted by CSE and have either been fully implemented or are at various stages of being implemented. Half of the remaining recommendations were accepted with some modifications or are very recent and are still being considered by CSE. The remainder were either bypassed by events or, in a few cases, not accepted by CSE.[80]

The office's impact on the public and parliamentary practice has, however, been extremely limited. In large part, this has been due to the rather innocuous nature of its public reports, especially in its early years. Perhaps for this reason, only one commissioner has been called to testify on the office's annual reports, which have also garnered scant media attention.[81]

Senate committees

An examination of the work of the Senate on matters of national security since the establishment of CSIS suggests that its committees have been far more robust than committees of the Commons in scrutinizing the work of Canada's secret world, despite not having the right to have their reports responded to within a set period by the government. They have produced many

more substantive reports than their counterparts in the House. This is true of both Senate special committees and Senate standing committees. Noteworthy among the former are the two committees dealing with terrorism in the 1980s that were chaired by Senator William Kelly and his Committee on Security and Intelligence of the late 1990s. Similarly, the Senate's Standing Committee on National Security and Defence, chaired by Senator Colin Kenny, has been particularly active in this regard, providing some 16 substantive reports since 2002. And whereas the work of the House has on balance tilted toward matters of propriety, the Senate's committees have been more broad-brush and have tended to be more interested in matters of efficacy, particularly concerning the capacities of the various members of Canada's national security apparatus and their performance. While one may sometimes disagree with the style, the frequently alarmist tone and the approach taken by the Kenny committee, and even with some of its findings, one cannot dispute the fact that it has continuously raised the profile of a wide spectrum of security concerns of national importance, something that House committees have largely failed to do.

The office of the auditor general

One of the most important bodies created during the period following Confederation, from Parliament's perspective, was the Office of the Auditor General of Canada. This body has been independent of the executive branch since its establishment in 1878. The vast majority of review bodies – even those said to be independent – keep to the convention of ministerial responsibility by reporting to the responsible minister, who then tables their annual reports in Parliament. In stark contrast, the auditor general's reports are referred directly to the Public Accounts Committee, one of only a few committees to be chaired by a member of the official opposition. Besides conducting comprehensive audits of individual departments and agencies, it also conducts value-for-money audits of specific programs and government-wide issues. It therefore can provide invaluable insights for members of Parliament regarding the efficacy and finances of government organizations.

Although the McDonald Commission made brief reference to the desirability of ensuring financial accountability for national security through the OAG, the *CSIS Act* made no specific provision for such financial audits. However, in the mid-1990s, at the urging of the special committee that had reviewed the *CSIS Act*, in the context of federal expenditure reduction and systematic program review following the end of the Cold War, the OAG initiated the first audit of Ottawa's security and intelligence functions as a whole. This report, which was to become the first of a regular cycle and specifically focused on control and accountability across the intelligence community, was unprecedented in scope. The US Government Accountability Office has audited specific programs, but never the entire field of intelligence.[82] The OAG was highly specific in recommendations for tightening controls and modifications to address indicated weaknesses.

In recent years, reports from the OAG have attracted increasing public attention, and governments appear to be under more pressure than in the past to respond positively to shortcomings revealed by the audits. The OAG is specifically mandated to examine financial controls, cost-effectiveness of government operations and standards of public service ethics in handling the taxpayers' dollars. These are important factors to consider in national security accountability, and the OAG is qualified to carry out such reviews, particularly given its practice of revisiting programs with a view to establishing whether improvements have been made.

In 2003, the OAG released a report specifically directed at gaps in the extent and nature of the external review of Canada's security and intelligence agencies, and in the disclosure of findings. The OAG assessed the level of external independent review over each agency involved either directly or in providing assistance with the collection of intelligence within Canada, including CSIS, the RCMP, National Defence, the CSEC, the Canada Revenue Agency (CRA) and the Financial Transactions and Reports Analysis Centre of Canada (FinTRAC). The OAG concluded that powers to review security and intelligence agencies vary widely.[83] With respect to the Canadian Forces, the CRA and FinTRAC, the OAG noted that the organizations do not have a specific agency that independently reviews compliance with law and ministerial direction.[84] With respect to the RCMP, the OAG concluded that the Commission for Public Complaints against the RCMP does not have the same level of access to RCMP information as the inspector general and SIRC have to CSIS information. Just as review agency mandates vary, so too do the reporting and disclosure of findings to Parliament. The OAG recommended that the government should assess the level of review in reporting to Parliament for security and intelligence agencies to ensure that agencies exercising intrusive powers are subject to levels of external review and disclosure proportionate to the level of intrusion.[85]

Recent reviews by the OAG include a critical audit of the effectiveness of the anti-terrorism initiatives after 9/11, which received wide publicity in and outside Parliament.[86] In April 2005, the OAG reported on a wide-ranging and critical review of the Canadian Air Transport Security Authority, the Crown corporation responsible for airport screening. In this context, Auditor General Sheila Fraser specifically commented on the challenges Parliament faced in holding the government to account for security and intelligence matters, particularly where the mandates of a number of government departments and agencies overlap. While she acknowledged that key information had to be kept secret, the Auditor General observed that Parliament also needed to be able to scrutinize the spending and performance of security and intelligence activities. In her view, it needed to receive reports containing classified information from security and intelligence agencies as well as organizations such as her office that are charged with scrutinizing such agencies on Parliament's behalf.[87]

Ad hoc review forms

Apart from the permanent institutional devices we have been describing, national security activities have also called into being a number of ad hoc or one-time-only efforts at review or assessment. Most notably, the various public inquiries called by successive governments over the years are key players in shaping and developing accountability systems. But the quest by governments for advice in this area has not been limited to public inquiries. In the 1980s, under the Progressive Conservative government, two national security issues precipitated serious internal reviews. The first was the tragic bombing of Air India Flight 182 on June 23, 1985, which constituted the largest mass murder in Canadian history and the most deadly attack involving an aircraft anywhere prior to 2001. While strenuously resisting a public inquiry and discouraging both SIRC and Parliament from considering the matter, supposedly to avoid jeopardizing the RCMP's criminal investigation, the government tasked the Interdepartmental Committee on Security and Intelligence under a senior public servant, Blair Seaborn, to undertake a review of aviation security. Focusing strictly on efficacy issues, his report (Seaborn 1985) is believed to have played an important role in shaping the aviation security regime for the next decade and a half.[88]

The second review arose out of strong criticism by SIRC of the Cold War-style Counter-Subversion Branch in CSIS. Apparently, too many Canadians were being put under surveillance, either because they were members of a targeted group or because they had come into contact with someone who was already under surveillance. Instead of choosing between CSIS and the advice of its review agency, the solicitor general appointed a task force headed by a retired senior public servant, Gordon Osbaldeston, to investigate the problems experienced by the newly civilianized security service. Osbaldeston's advice, which was made public, coincided with that of SIRC and the inclinations of the solicitor general, but added independent legitimation (Independent Advisory Team on the Canadian Security Intelligence Service 1987; Gill 1989). Few independent review bodies have been as successful: the vast majority of its recommendations were accepted. Furthermore, the Counter-Subversion Branch was ordered closed, an important step in the evolution of CSIS.

More recently, other forms of review have been initiated in the aftermath of 9/11. Since the passage of the *Anti-terrorism Act*, the government has experimented with a form of quasi-nongovernmental advice on its national security policies. Two advisory panels made up of nongovernmental people have been created to meet on a regular basis to review policy and performance. The National Advisory Council on National Security (modelled to a degree on the US president's Intelligence Advisory Board) consists of a panel of independent experts on security and intelligence. The Cross Cultural Round Table on Security draws on representatives of Canada's various cultural communities to provide government with minority experiences and perspectives – in practice, no doubt, with special attention to the Muslim and Arab communities that are most affected by the current counterterrorist emphasis in national security. It is too early to know what impact these bodies have had.

The enactment by Parliament in 2002 of the *Canadian Air Transport Security Authority Act* established CATSA as a Crown corporation. The legislation's principal purpose was to provide an improved and standardized mode of screening at Canadian airports of air passengers and their checked luggage and on-board belongings before they travelled within Canada or abroad. Another major initiative was the screening of non-passengers at Canadian airports. Since its inception, CATSA has undergone two major reviews. The first was conducted by the OAG. The second concerned a review of the legislation itself. Instead of following the normal practice of having the statute reviewed by Parliament, the Act provided

for a five-year review of the new agency's mandate and performance by the minister. The government chose to conduct this review by appointing an independent advisory panel to the minister of transport with a mandate to review not only CATSA but aviation security in Canada in general, and to report to the Air India inquiry on the aviation security aspects of that tragedy. The panel's report was made to the minister, and then tabled in Parliament (Advisory Panel on the Review of the CATSA Act 2006).[89] This report and CATSA's annual reports, which are public documents but not specifically tabled in Parliament, have received limited attention by Parliament.

In April 2007, the government appointed an independent investigator to examine allegations of mismanagement of the RCMP's pension and insurance plans. Ordinarily such a matter might have been of relatively minor importance. However, the investigator's June 2007 report, entitled *A Matter of Trust*, found broader problems that would have further ramifications. In investigator David Brown's opinion, the RCMP's management system was "horribly broken," with a command-and-control culture that was exercised by an "autocratic leader" who punished whistleblowers. Two factors were responsible for permitting the RCMP's paramilitary structure to go unchecked. These were "the absolute power of the Commissioner and the absence of meaningful oversight of his management style." Instead of making specific recommendations to resolve specific issues relating only to the pension fund scandal, Brown recommended that a task force be struck to produce a major fix before rank-and-file morale was sapped further (Clark 2007). The government responded by doing exactly that.

When the Task Force on Governance and Cultural Change in the RCMP reported at the end of the year, it made three fundamental recommendations. First, the RCMP should be established as a separate entity from government with separate employer status, just as is the case with CSIS. In this way, it would be able to manage its financial affairs and human resources properly. Second, because the task force believed the RCMP would need to build capacity at nearly every level within the force, a new civilian board of management would be required to provide overall stewardship of the organization. This would include oversight of financial affairs, personnel, property, procurement, resources and services. The board would be accountable for the organization to the minister. Such a level of independent responsibility needed to be balanced with increased accountability and transparency. In this regard, the task force believed that the separation of the Commission for Public Complaints from the External Review Committee, which deals with internal matters of discipline and complaints from RCMP members about their working conditions and so on, was inadequate, with neither body having sufficient authority to compel real action. To rectify this situation, the task force recommended the creation of an Independent Commission for Complaints and Oversight of the RCMP. This body would be established by statute, have official independence and report publicly. It would have all the existing functions but would have authorities consistent with those of an ombudsman. It would have the powers to consider complaints, initiate investigations, summon witnesses and compel testimony, with its recommendations binding on the RCMP commissioner.[90] Although the government appointed its first civilian commissioner shortly after the independent investigator's report was published, it has yet to initiate responses to the task force's recommendations. Moreover, some of the recommendations are at odds with those of the Arar Commission's policy review, discussed in detail below, to which the government also has yet to respond.

Yet another form of ad hoc review was the Independent Panel on Canada's Future Role in Afghanistan, chaired by John Manley, which reported in 2008. From the government's point of view, this review, which was surprisingly silent on the role of intelligence in counter-insurgency, had the specific purpose of gaining a parliamentary majority for an extension of the military mission in Afghanistan, which was accomplished with the support of the official opposition. The Manley report also contains some critical reflections on the government's performance. This latter element points to a structural problem with all such ad hoc reviews: after they are made public, there is no automatic or compulsory requirement for government to respond to specific recommendations or advice, or to provide answers to why specific recommendations have been rejected or ignored. This is often the case with public inquiries, leading former commissioner John Gomery to castigate the government for ignoring many of his recommendations from his inquiry into the sponsorship affair. One answer to such concerns might be to establish a procedure whereby the government that called inquiries or reviews would be under an obligation – not, of course, to accept all or any of the recommendations, but to provide an answer to Parliament on its response within a specified period of time.

In 2005, Parliament adopted the *Public Servants Disclosure Protection Act* to cover would-be whistle-

blowers. It protects public sector employees from liability that may result from disclosing information about wrongdoing. While most elements of the security and intelligence community are covered by this legislation, including review bodies, both CSIS and the CSEC are specifically exempted. They are, however, required to establish similar procedures for their specific organizations. The CSE commissioner is also obliged under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy should they wish to claim a "public interest" defence for divulging classified information.

A committee of Parliament or a committee of parliamentarians?

One of the Martin government's initiatives was to address what it perceived as the "democratic deficit." Among its recommendations to offset this deficiency was a proposal to establish a parliamentary committee to scrutinize Canada's security and intelligence community. A subsequent government policy paper, however, recommended instead a committee of parliamentarians along British lines (Glees, Davies, and Morrison 2006). A committee of parliamentarians, although made up of MPs and senators, would not be a committee of Parliament capable of exercising traditional parliamentary rights and privileges. It would be established by statute, have its membership appointed by the prime minister and exercise only such powers as the statute stipulates. Furthermore, if the British model were followed, the committee would likely have its staff drawn from the public service, not from the Library of Parliament's Research Branch, a nonpartisan body independent of the executive.

The case for a committee of parliamentarians over a parliamentary committee rests on the belief that broader access to documents and people in government would be facilitated, that secrecy might be better assured and that partisanship could be minimized. The arguments in favour of a committee of Parliament stress the importance of maintaining effective parliamentary scrutiny of the executive-dominated national security field.[91] We assess the alternatives in our concluding section of policy recommendations, below.

In any event, the Martin government fell before its proposal could be implemented. The current government has indicated that it too would follow through on appointing some form of committee. This promise has yet to be met as the government contemplates a wider range of current accountability recommendations, discussed in the following section.

The Post-Arar Accountability Reform Agenda

In the post-9/11 environment, a familiar rhythm has returned once again to the evolution of national security accountability: a security scandal has led to a special public inquiry, followed by a proposed reform agenda for an existing accountability regime that has been found wanting under pressure. Once again, the focus has been on propriety rather than on efficacy, or even on both considered together. The scandal was the "extraordinary rendition" of Maher Arar, a Canadian citizen abducted by US authorities while in transit at a New York airport and sent to Syria, where he was held in confinement and tortured before his release almost a year later. Justice Dennis O'Connor was eventually appointed to lead a commission of inquiry, known as the Arar Commission, into the facts surrounding the possible complicity of Canadian officials. The inquiry's terms of reference included a second part that mandated O'Connor:

> (b) to make any recommendations that he considers advisable on an independent, arm's length review mechanism for the activities of the Royal Canadian Mounted Police with respect to national security based on (i) an examination of models, both domestic and international, for that review mechanism, and (ii) an assessment of how the review mechanism would interact with existing review mechanisms.[92] (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar 2004)

Actions by the RCMP lay at the heart of events leading to Arar's ordeal. As noted earlier, the RCMP had entirely escaped accountability for its continuing national security activities when CSIS was created with its new accountability regime. The RCMP Commission for Public Complaints, established after the *CSIS Act*, failed to meet the challenge of the Arar scandal. Arar offered an opportunity to expand accountability to include for the first time a leading player in Ottawa's national security activities, one made even more important by the *Anti-terrorism Act*, which had criminalized forms of behaviour previously not subject to law enforcement and had made the RCMP a leading force in integrated anti-terrorist investigations. O'Connor chose to interpret his mandate as calling for recommendations on national security review across the entire institutional spectrum, rather than exclusively focusing on the RCMP. Thus, O'Connor offered a system-wide reform of

national security review rather than a narrowly institution-bound prescription, but one that did not consider a role for Parliament.

In pursuing a wider scope, O'Connor was addressing a key new feature of national security activities in the post-9/11 environment: integration of anti-terrorist efforts – across federal agencies and departments, across governments in Canada and across borders in joint activities with allies. Since the terrorist threat is said to be borderless and globally networked, effective counterterrorist responses must overcome traditional institutional and jurisdictional "stovepipes." CIA-FBI conflict had contributed to the intelligence failure of 9/11, as the US 9/11 Commission had found (National Commission on Terrorist Attacks upon the United States 2004). In Canada, turf wars between the RCMP and CSIS had contributed to the failures both to prevent the 1985 Air India bombing and to prosecute the alleged perpetrators. These lessons were now being addressed by the agencies charged with counterterrorism, and by an unprecedented (but perhaps still inadequate) degree of interagency cooperation.[93] The new investigative philosophy promises greater effectiveness but also presents a problem in designing a new review system focused only on an RCMP that is increasingly operationally integrated in an institutional sense with other players in the process, including those at the provincial and municipal levels and outside Canada. A distinct danger to avoid is the lowering of investigative standards in criminal cases where prosecution, not intelligence gathering, is the aim, which might be brought about by the possibility of information being derived from intelligence agencies operating under different and lower investigative standards.

The Arar Commission also recognized that the RCMP was following a trend among law enforcement agencies throughout the Western world by adopting a model of intelligence-led policing. In the area of national security, the RCMP would be expected to engage in intelligence gathering in close collaboration with other agencies, both domestic and foreign, that were primary intelligence producers. This makes drawing clear lines of accountability focused along institutional boundaries more problematic than in the past.

The principle of police independence with regard to criminal law enforcement, which continues to account for most of the RCMP's time and resources, presents certain difficulties in establishing greater accountability for the force's national security activities, which themselves form a relatively small proportion of its overall workload. This was of course the reasoning behind the separation of the security service from the RCMP in 1984. The RCMP and the government have recognized that the arm's-length relationship regarding criminal law enforcement cannot and should not be maintained with regard to national security investigations. Indeed, ministerial directives guide the RCMP in its conduct of national security investigations. But external review of the RCMP's national security activities faces the problem of applying a mechanism created with one kind of activity in mind to an agency most of whose activities do not correspond with this focus and follow a different set of rules with regard to relations with government.

When O'Connor chose between review options, a non-starter was the status quo: that is, leaving the RCMP Commission for Public Complaints (CPC) in place under current rules. This body had failed to deal with the Arar affair, and the former chair of the CPC was on the public record describing the existing process as dysfunctional (Sallot 2005; Shephard 2005).[94] If the CPC were to remain in place, it would have to be beefed up with powers appropriate to an enlarged post-9/11 workload and shorn of the weaknesses in the existing body. Other options would still have to address the issue of the integration of RCMP national security activities with other agencies.

A "Super SIRC" option was discussed, in which SIRC would be expanded beyond its institutional focus on CSIS to include the RCMP and other agencies engaged in national security operations. SIRC might be a model that, with appropriate additional resources and enlarged powers, could provide external review of national security operations on a functional, rather than institutional, basis. In effect, a "Super SIRC" could replace the CPC, perhaps replace the CSE commissioner and expand its review capacity to the national security activities of all government departments and agencies with a national security footprint. This was the preferred option of the outside experts consulted by the Arar Commission, as well as of the public intervenors who testified and presented written submissions. The reason most often advanced for this preference was improved accountability for propriety, although the potential of a more comprehensive spotlight on all national security activities was also indicated.

Ultimately, O'Connor judged this option to be unrealistic. Despite its emphasis on integrated operations, the government had not actually integrated the various agencies engaged in national security into a single con-

solidation of CSIS, the RCMP, the CSE and other entities, but was relying instead on improved mechanisms for cooperation and communication between existing agencies while retaining their separate identities and mandates. As a result, it was thought that external review might be better designed if it mirrored these institutional arrangements and permitted agency-specific review bodies to learn with experience the organizational culture of the bodies they are reviewing.

The Arar Commission recommended a solution that marries the advantages of government-wide review of national security with the advantages of a dedicated institutional focus. Keys to this compromise include the concept of "statutory gateways" that permit a review body to follow a trail of evidence from one institution to another, and an institutional innovation: a committee to coordinate the activities of the existing review bodies and offer a single focus of entry to the complaints process for the public.

The old Commission for Public Complaints against the RCMP would be significantly restructured as the Independent Complaints and National Security Review Agency (ICRA). ICRA would have the ability to conduct self-initiated reviews; investigate complaints; conduct joint reviews with SIRC and the CSE commissioner into integrated operations; and conduct reviews upon ministerial request. ICRA would have investigative powers similar to those under the *Inquiries Act*, including the power to subpoena documents and compel testimony, initiate research and conduct public education programs. Taking account of the principle of police independence, ICRA would also have the "power to stay an investigation or review because it will interfere with an ongoing criminal investigation or prosecution" (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar 2006a, 539).

Complaints could still be referred to the RCMP for investigation, but a complainant could request that ICRA conduct the review itself. Both the complainant and the RCMP would have the opportunity to make representations at hearings. In the case of national security confidentiality, ICRA would have discretion to appoint security-cleared counsel independent of the government to test the need for confidentiality.

ICRA would issue a report annually to the minister, a disclosable version of which would be laid before Parliament, and would also issue a report to the minister on its self-initiated reviews and complaint investigations.

O'Connor identified five departments or agencies of the federal government with significant roles in national security that should be subject to review: Citizenship and Immigration Canada, Transport Canada, FinTRAC and Foreign Affairs would be designated to have their national security activities reviewed by SIRC. The Canada Border Services Agency (CBSA), which exercises some law enforcement powers, would be reviewed by ICRA. Omitted from this list were the Privy Council Office (PCO) and its International Assessment Staff (IAS), which, though having no investigative or coercive powers, might have been included because their efficacy has sometimes been questioned.[95]

"Statutory gateways" among the national security review bodies would provide for exchange of information, referral of investigations, conduct of joint investigations and coordination in the preparation of reports. A new body, the Integrated National Security Review Coordinating Committee (INSRCC), comprising the chairs of ICRA and SIRC and the CSE commissioner, with an outside person to act as chair, would have a mandate that would include making sure the statutory gateways operate effectively; avoiding duplicate reviews; providing a single intake system for complaints; reporting on accountability issues and trends in the area of national security in Canada, including the effects on human rights; conducting public information programs; and initiating discussion for cooperative review with review bodies for provincial and municipal police involved in national security activities. Significantly, O'Connor recommended that "an independent person" – not Parliament – be appointed to review the new framework after a period of five years (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar 2006b, 22).

In assessing O'Connor's recommendations, it is crucial to note that he explicitly foreclosed discussion of review for efficacy, in favour of a narrower focus on propriety alone, which he took to be his particular mandate. The Arar Commission falls into the familiar pattern of scandal eliciting reforms that focus more on propriety (whether the agency acts in accordance with law and ethical standards) but less on the efficacy of the agency's activities (whether its activities are in accord with the policy objectives of government). O'Connor interpreted his mandate as a review primarily for propriety: "It was concern about the propriety of actions taken with respect to Maher Arar that gave rise to this Inquiry." Thus, he did not conduct the inquiry "with the goal of making recommendations about the efficacy of the RCMP's national security

activities, and I am therefore not in a position to evaluate whether an independent review mechanism is needed from this perspective." He does go on to admit that "issues of efficacy and propriety are interwoven" and that "while efficacy will not be the primary objective of the review mechanism I recommend, it will in many cases be a necessary element of a robust review for propriety" (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar 2006b, 467).

This constitutes a serious shortcoming in the recommendations for new review procedures, in that those conceived by O'Connor apply only to matters of propriety. In this regard, the commission made a distinction between review and oversight, terms it defined in a particular way. To O'Connor, review meant examining operations after the fact, as opposed to oversight, which he interpreted as including a degree of involvement in ongoing investigations. The latter course was rejected, for a variety of reasons, most convincingly because of concern about the reviewers becoming entangled in the evidentiary trail they are supposed to review. Review for propriety is concerned with identifying illegal or unethical actions and might thus be considered a quasi-judicial function. As such, it is important that those carrying out the review have no prior involvement in the matters being reviewed. To take a hypothetical example: if a review body was regularly notified of ongoing surveillance targets, its capacity to impartially review a complaint regarding surveillance might be called into question. Thus, almost all the review envisaged in the O'Connor report is *ex post facto*, with only minor exceptions where some reference to continuing investigations may be unavoidable. While this may be appropriate for propriety reviews, which demand a degree of quasi-judicial impartiality, it is unlikely that review for efficacy will be effective without some involvement by the reviewers at earlier stages in the process.

The extension of accountability to include the national security activities of the RCMP is long overdue, and indeed should have formed part of the 1984 reforms. It was always a fallacy to imagine that separating security intelligence from law enforcement and subjecting only the former to effective accountability could resolve the fundamental issues.[96] In any event, rising demands for RCMP accountability in criminal law enforcement have become irresistible. The appointment of the first civilian commissioner, with a mandate to impose greater transparency, and external probes into internal conflicts in the RCMP (as detailed above) all point toward the imposition of some stronger form of accountability, of which national security review will be one part.

Another timely and important contribution is the emphasis on cross-institutional integration of national security activities and the requirement for accountability to reach across narrow institutional boundaries. Whether the solutions offered by O'Connor constitute the best practices remains to be seen, but they are the only ideas yet on offer from any officially sanctioned inquiry. There were two after the Arar Commission: the Iacobucci Internal Inquiry, which had no mandate to review policy, and the commission of inquiry into the 1985 Air India tragedy, which has yet to report, but in any event is focused on the situation more than two decades ago.

There are a number of gaps and limitations in the Arar Commission's policy recommendations. For one, O'Connor interpreted his mandate as excluding consideration of a proposed national security committee of parliamentarians or a standing committee of Parliament. The question of how the proposed changes would fit with an expanded and enhanced parliamentary role is essential.

The failure to address review for efficacy has consequences. In recent years, some of the most crucial questions that have required external independent review have been precisely those of efficacy arising out of catastrophic intelligence failures. For example, the 9/11 attacks in the US caused the 9/11 Commission to focus on the inefficacy of US intelligence and to recommend reforms to address these serious deficiencies (National Commission on Terrorist Attacks upon the United States 2004). In Canada, the Major Commission on the Air India tragedy is almost entirely focused on the efficacy rather than the propriety of Canadian national security. An earlier SIRC investigation into Air India was postponed at the request of the government until it was no longer timely, a poor reflection on SIRC, as its first chair, Ron Atkey, has subsequently admitted (Clark 2005).

Ironically, in the one place where O'Connor refers to the proposed parliamentary committee, it is to suggest that it might be a more appropriate venue for efficacy reviews, thus potentially tying together the two most obvious pieces of unfinished business in his report (Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar 2006b, 467). This offers an appropriate place to move toward our conclusions on the state of accountability in national security and our policy recommendations for the future. The Harper Conservative government, which accepted unreservedly all the recommendations of O'Connor's factual inquiry and quickly set about acting upon them, has yet

to respond to the recommendations of the policy review, or even to give any clear signal of its intentions. Therefore, the future shape of accountability remains open to policy advice.

What We Know about the Current System of Accountability

At the beginning of this paper, we put forward a series of questions about the nature of current accountability procedures, with a view to establishing the degree to which they have made Canada's security and intelligence community understandable, transparent and public. Below are some brief assessments.

Alhough the accountability procedures are complex, we cannot talk about the existence of a system or network of accountability procedures, for two main reasons. First, there are poor linkages between many of the key elements. While the lack of good connections between Parliament and the various review bodies established by statute is most noticeable, the same deficit has been evident in the past among review bodies themselves. Though Parliament has the legal authority to call anybody to testify and to expect honest answers, full responses to questions have not been the practice. Even when independent review bodies have come before Parliament, they have felt restrained in their capacity to respond to questions in any really detailed way. Such was the case, for example, with SIRC at the time of the five-year review. Also, the Auditor General is on record as saying that Parliament must be able to receive classified information from her. In the case of SIRC and the IG, both of which report initially to the minister, until recently the timing of their annual reports often meant that the IG's certificates were not considered by SIRC in time to be included in SIRC's report for the same year. While this problem appears to have been rectified, the addition of new review and oversight bodies may produce similar problems in the future.

Second, while some institutions are scrutinized by several different bodies, others either are scrutinized by a single institution or remain completely out of the spotlight. CSIS, for example, receives considerable attention from both SIRC and the IG. By comparison, the CSEC is reviewed by one body, once a year. Still others such as the IAS, most of National Defence and the CBSA receive no external independent review on a regular basis. Furthermore, when it comes to conducting such scrutiny, review bodies may not in practice see everything the law suggests they should. Parliament, for example, has been prevented from seeing certain things because it could not guarantee that they would remain secure. Similarly, SIRC has sometimes been prevented from seeing certain information because it originated from a foreign intelligence service.

There are three key divides among the procedures that are in place. The first is between those procedures that operate outside the executive branch and those that operate inside it. The purpose of the latter appears to have more to do with ensuring sound control and management practices; those outside vary considerably in their strategic objectives. Some, such as the judicial approval of warrants, are designed to ensure that particular intelligence-gathering techniques fall within the law. Others are there to scrutinize particular practices and to provide accounts to various political actors – officials within the executive branch, members of Parliament, other review bodies, the media and the public at large. Still others investigate public complaints and make recommendations regarding policy.

Another important divide concerns propriety and efficacy. Some review bodies like the Office of the CSE Commissioner have a statutory remit that looks only to the propriety of past actions. Some, such as SIRC, have a responsibility for both. A third group, which would include certain commissions of inquiry, have examined only efficacy issues. In all cases, what appears to be missing is bodies that can examine matters adequately before the fact. This applies to issues of propriety, where review bodies are not explicitly required under their mandates to evaluate on an annual basis whether the existing applicable laws are adequate. This is particularly important where changes in technology or agency mandates are concerned.

A final divide concerns institutions that are permanent and those that are temporary. Most of the independent external review bodies are now established by statute. There are exceptions, however, to this general rule. The House of Commons Subcommittee on National Security could easily be disbanded by its parent, the Standing Committee on Justice and Human Rights, or have its terms of reference changed. Similarly, the approach of the Senate's Standing Committee on National Security and Defence might easily change with a different chair. By comparison, most of the current internal accountability mechanisms have been established through policy initiatives rather than by statute. There are

also exceptions, the IG being one, to this general rule. Many of the accountability mechanisms that have been used are of a temporary nature. Commissions of inquiry, task forces and independent panels, which are all normally established by executive order, die with the completion of their reports, as do statutory reviews of legislation by parliamentary committees or the work of special committees once completed. While Parliament may of course take up any matter it chooses, it seldom does go back over such completed work, leaving it instead to be reviewed by others, sometimes by the auditor general where appropriate. This is unfortunate as the terms of reference of such bodies are normally set by executive order and may not be of the widest remit. Recent commissions of inquiry suggest, in fact, that closer scrutiny needs to be given to such terms of reference, not only for the breadth of their obligations but also for how they have been interpreted.[97] There is now only an obligation on the part of the executive branch to respond to House of Commons committee reports within a set time. Arguably, there is a need to follow up all such reports, as well as Senate committee reports, after a reasonable period to establish how the government has responded to their various recommendations.

We can also point to a fundamental gap in the overall system. There is no single body outside the executive branch with the capacity or responsibility to examine the whole security and intelligence community for both its efficacy and propriety. Arguably, this is of crucial importance as there are a growing number of areas where many elements of the community need to work together; the provision of security for the 2010 Olympic games in Vancouver-Whistler and support for Canadian Forces in Afghanistan are good examples. In such instances, there needs to be consistency of policy, coordination of the analytical process and general collaborative effort. The OAG answers to this description best, but its purview extends only to the efficacy aspects of organizations. Similarly, on the propriety side there are several ombuds-like offices. But these deal only with very specific dimensions – human rights, privacy, access to information, official languages – of organizations across government.

This gap in the overall system also means there is no body that can evaluate whether all the various review bodies are working as their instigators intended. In fact, there have been clues in the past suggesting that all was not well. The five-year review process found an example of SIRC exhibiting poor research methods. Given that there has been no external attempt since 1990 to re-evaluate SIRC's methodologies, it is impossible to tell whether this was a mere aberration or something more serious. Similarly, during the five-year review process, when faced with a special committee that tended toward recommending collapsing the role of the IG into SIRC, the Minister impressed on the special committee the importance of the work provided by the IG. Yet at least two inspectors general subsequently ran into difficulties fulfilling the office's mandate, failing in this regard to receive adequate support from their minister; at one point, the office was left vacant for over a year. It is thus difficult to gauge whether a separate office really is necessary or whether subsequent incumbents have been co-opted by CSIS. In addition, the gap means that there is no body that evaluates what has happened to all the recommendations that the various review bodies have made. True, each of them can revisit its recommendations in subsequent annual reports, but their capacity to effect change, particularly where it relates to more than one national security agency, is limited.

Many of the problems identified above might be resolved through a much greater parliamentary role. But we are under no illusions that this will be an easy matter. Parliament has its own organizational culture, one that at best is ambivalent toward security and intelligence scrutiny. As indicated, the conflicted role that parliamentarians perform – to support or oppose the government on the one hand, versus scrutinizing government activity on the other – is not necessarily conducive to the careful analysis of the secret world with a view to establishing whether it operates both to protect national security and in the interests of all Canadians. To be sure, we can expect most parliamentarians to deal with "fire alarms" but not necessarily to do the "police patrolling" type of oversight that is necessary. But not all legislators are likely to approach their work from the same perspective. As Loch Johnson has recently suggested, legislators may approach the scrutiny of intelligence from quite different perspectives. He classifies them as "ostriches" (those demonstrating a benign neglect toward intelligence agencies); "cheerleaders" (those who act as "boosters" for the intelligence community); "lemon suckers" (those who are inherently skeptical of both intelligence practices and the value of intelligence); and finally "guardians" (individuals who are both partners and critics of the intelligence community). Furthermore, he posits that particular overseers have fluctuated between these various identities (Johnson 2008). The trick, therefore, will be to find sufficient numbers of individuals who are consistently prepared to act as "guardians."

Conclusions and Policy Recommendations

One observation that may readily be drawn from our discussion of the concept of accountability and of the evolution of the various procedures developed in Canada to make national security activities of the federal government accountable is that this is a matter of considerable complexity. There is no single, generally agreed-upon definition of accountability; instead we find it more useful to speak of "accountabilities," a number of mechanisms, each of which answers differing questions depending on the political, institutional and cultural context and on the specific issues giving rise to demands for greater accountability. Forms of accountability in national security have arisen in Canada in answer to specific concerns, often voiced in a context of public controversy, and have developed in an ad hoc, piecemeal and uncoordinated fashion, resulting in a complex patchwork that defies easy rationalization around coherent principles. Significantly, certain organizations within Canada's security and intelligence community and their practices routinely go unexamined. Overall, the systems of accountability emphasize propriety over efficacy.

It would be futile to seek accountability per se, as a good in and of itself. Indeed, as the aftermath of the sponsorship affair and the Gomery Commission testify, the quest for greater accountability as an end in itself may have perverse effects on the operations of government. Instead, we should begin by asking the fundamental questions: Why accountability, and for what?

As we have seen, historically the quest for greater accountability in national security has been driven most often by concern over impropriety. The exercise of extraordinary powers, cloaked in unusual levels of secrecy, has from time to time given rise to anxieties over abuse of these powers and the potentially negative impact on human rights, civil liberties and the fabric of liberal democracy.[98]

The McDonald Commission laid the basis for the most significant policy response to concerns about propriety. The *CSIS Act* and new accountability processes for CSIS followed. The Arar Commission has demonstrated that this agenda is by no means exhausted. The failure to provide effective accountability for the RCMP's national security activities demonstrated the incomplete, patchwork quality of the accountability architecture previously erected. Moreover, O'Connor has pointed in his recommendations to the broader unfinished business of accountability for propriety by calling for mechanisms that better integrate review of national security operations, which are increasingly integrated across jurisdictional lines, both within the federal government and between the federal and other governments. O'Connor's recommendations for an enhanced and effective RCMP complaints body, along with a system of statutory gateways among the review bodies and a new Integrated National Security Review Coordinating Committee to direct traffic between the review bodies, are the best proposals on the table and should be implemented by the government as part of its expected response to the second part of the Arar Commission report.

The unfinished business of review for propriety is important to keep in mind, but it is crucial that attention to this relatively well-worn reform agenda not distract attention from bigger pieces of unfinished business, two of which we would particularly single out: the almost untouched matter of accountability for efficacy; and the poorly answered question of accountability to whom, particularly to Parliament, as well as to the executive branch.

The persistent emphasis on propriety has meant, not surprisingly, that greater attention has been paid to the collectors of intelligence – those on the sharp end of the process, with the capacity to intrude on civil society and intimidate and coerce. Perhaps as a consequence, several elements of the intelligence community that do not participate in intelligence collection within Canada are not routinely considered. Examining for efficacy would require a much broader remit covering the capacity and performance of all bodies with a role in national security and intelligence.

The concern over propriety has certainly been justified, and will continue to be justified, by the very nature of national security activities. Yet propriety issues, taken in isolation, can be misleading guides. The McDonald Commission was well aware of this. The famous and delicate balance to which McDonald pointed was between freedom and security. Most of the problems that inquiry had to address were the result of the balance being tipped too far against freedom in the name of security, and their recommendations attended mainly to restoring that balance. Yet, as the McDonald Commission stated, "Canada must meet both the requirements of security and the requirements of democracy: we must never forget that the fundamental purpose of the former is

to secure the latter...Canada must have effective security. Security measures have the basic objective of securing our democratic system" (Commission of Inquiry concerning Certain Activities of the Royal Canadian Mounted Police 1981, 1:43, 47).

Democracy can be undermined by unchecked pursuit of security. Yet security can be undermined by exclusive concern with democratic freedoms. In the contemporary era of terrorism, inadequate security could mean that citizens might suffer the worst possible violation of their human rights, the loss of their very lives (as indeed happened to the victims of the Air India bombing in 1985). But more to the immediate point, in order to strike the appropriate balance, Parliament and an informed citizenry must be able to assess not only the freedom side, but also the security side. Accountability must encompass not only propriety issues but also efficacy issues. Is security being adequately protected? Are the agencies charged with this responsibility doing an effective job? Is the public receiving value for money? What needs to be done to improve security? These questions may be addressed by the various external review agencies already in play, such as SIRC and the OAG, as well as internal reviewers like the IG for CSIS; or by parliamentary committees like the Senate committee on national security under Colin Kenny; or by occasional public inquiries. How adequately they have been addressed is another matter. There certainly are doubts about the erratic quality of such inquiries, the failure of overall direction and coordination, and the lack of continuity.

But there is a deeper problem. These specific efficacy questions fall within the larger question of national security policy. Are the policy objectives set by government the correct ones? Are the agencies being usefully tasked? Has government used the intelligence and threat assessments it has received from its agencies appropriately? Once the line is crossed into matters of public policy, external review bodies become powerless. They must maintain policy neutrality or lose their apolitical status, and thus their legitimacy. There is only one body that has every right and duty not only to comment upon but also to participate in the making of public policy, and that is Parliament. Recall that O'Connor in his policy review suggested that the two subjects he had deliberately neglected in his recommendations – review for efficacy and the role of Parliament – might fruitfully be combined.

There are reasons why Parliament should defer to external, independent, arm's-length review bodies for detailed and careful assessment of propriety issues. Investigations of complaints of possible impropriety, as well as assessments of whether national security activities are being carried out legally and ethically, call for quasi-judicial impartiality and political detachment on the part of the reviewers. It is no doubt unrealistic to expect that Parliament will voluntarily abstain from any intervention when "fire alarms" go off. The trick will be to have a system in which it holds back until after an independent review body has done its job. A watching and waiting role for Parliament in such instances would also ensure that the independent review body would not delay its investigation, as was the unfortunate case with SIRC and Air India. If there are clear advantages to political detachment in assessing propriety questions, when it comes to assessing efficacy, it is precisely political involvement that is required where public policy is fundamentally at stake.

To illustrate this point, we might take one well-known recent example from the US. The spectacular intelligence failure concerning the weapons of mass destruction allegedly held by Saddam Hussein's regime in Iraq was at the centre of the fateful decision to go to war in Iraq without international sanction. Was this failure the product of the intelligence agencies' own shortcomings, or was it, as many observers have concluded, the result of the administration pressuring the agencies to produce intelligence on demand to meet political objectives? Although inquiries by the US Senate Intelligence Committee in 2004 and 2006 faltered amid partisan considerations, there was no place where this tangled knot of political and intelligence issues could be more appropriately addressed than in Congress.

To take another example from the Canadian context, the failure of Parliament to address the efficacy of security and intelligence in the Air India tragedy in 1985 ultimately led to the calling of a public inquiry more than two decades later, long past the point when lessons learned could have been usefully applied, and in the context of long built-up resentment on the part of the victims' families at the apparent indifference of authorities to their losses. Given the importance of public policy considerations (the separation of CSIS from the RCMP; issues about intelligence being focused on Cold War versus terrorist targets) in assessing the intelligence failure, it is difficult to see any more appropriate body than Parliament to have carried out such an inquiry, not into the factual details but into the broad policy implications.

The proposal of the former Liberal government for a national security committee of parliamentarians has not yet been acted upon by the present Conservative gov-

ernment, although as a party the Conservatives promised to increase the participation of Parliament in national security matters. We take it as a given that some form of greater parliamentary participation will be brought forward in the near future. This is laudable in principle, but as always in institutional reform, the devil is in the details. There are certain conditions that must be met if Parliament is to play an enhanced role.

First is the relationship to Parliament of a national security committee. We do not endorse the idea of a committee of parliamentarians, as opposed to a committee of Parliament. Although the personnel of the former may be limited to parliamentarians, from the House or the Senate, it would be too much a creature of the prime minister, to whom the committee would report, if the UK model is any guide. The PM would appoint the members and determine how much of their findings and recommendations would be reported to Parliament. The PM would also select the staff for the committee (Phythian 2007: Davies 2002; Gill 2007). A committee of Parliament, on the other hand, would carry with it the rights and privileges of Parliament, which could, if exercised effectively, establish a degree of autonomy from the executive branch that would be crucial when reviewing the efficacy of national security activities carried out by the executive.[99] To be sure, the political difficulties surrounding the establishment of a relatively autonomous committee of Parliament during a period of successive minority Parliaments with attendant high levels of partisan competition should not be minimized. In this context, a committee of parliamentarians would no doubt be an easier sell to a government in office. But the principle of parliamentary autonomy is important to preserve.

Several countries have established such a committee, including both Australia and New Zealand. Our preference is something closer to the Australian model rather than that of New Zealand. Such a committee would be established by statute, have a broad remit with purview over the entire security and intelligence community, and have the capacity to report to Parliament at its discretion (but at least annually). This statute would also spell out the security procedures to be followed. Significantly, a committee established by statute would bind Parliament to doing a specific job on a regular basis. Thus, it would hopefully avoid the past inadequacies of ad hoc responses such as the Subcommittee on National Security.

A national security committee should be a joint committee of both House and Senate, which would indicate its special status and importance. The presence of senators could also lend greater continuity to membership, given the high turnover rate of MPs from election to election. The democratic legitimacy of elected MPs can be leavened with the relatively greater freedom from partisan ties of senators.

A committee of Parliament for national security should be seen as a special case among parliamentary committees. Most important, its members must have access to all relevant information, at whatever level of classification, and must therefore strictly abide by all the obligations of secrecy where required. Any committee staff must be security cleared to the same level as the staffs of external review bodies like SIRC. Committees must operate and deliberate under special security conditions that are higher than for those in effect for regular parliamentary committees. There is a price to be paid: members of such a committee will be to an extent "inside the loop" of the Ottawa security system. As such, they will inevitably experience limitations on their autonomy as parliamentarians to publicly discuss security policy and performance on the basis of all that they have learned as a result of their access to classified material. Remaining outside the loop, however, imposes the greater burden of irrelevance. Becoming partial insiders involves some trade-offs but is a necessary condition for meaningful participation in the process.

Another necessary trade-off would be required for effective operation of such a committee. Partisan considerations would have to be minimized. This need not imply in any way the muting or silencing of criticism of government policy and performance. A critical distance from the executive would be the *sine qua non* of effective parliamentary scrutiny of national security. But there is a significant difference between substantive criticism and partisan criticism. It is especially the case with regard to national security matters that partisanship must be minimized to the extent possible. In most areas of policy, partisan divisions are limited in their significance and ramifications for the wider political culture. When national security is at issue, partisan differences can quickly escalate into characterizations of loyalty and disloyalty to the nation. The US offers some unfortunate examples of the effects of the partisan politicization of national security issues, from the Cold War McCarthy era to the present era of the war on terror. Canada has been mercifully free of this malady for the most part, but there is a worrying example recently of a lapse into partisanship in the deplorable debate in the House on the extension of the preven-

tive arrest and investigative hearing provisions in the *Anti-terrorism Act*, in which allegations were traded of parties being "soft on terrorism" or "soft on Charter rights," to the detriment of any substantive discussion (Roach 2007, 9-11). Happily there are other more encouraging precedents, including the work of the special committee that conducted the five-year review of the *CSIS Act*, which, as described earlier, operated in an entirely nonpartisan fashion without limiting its capacity to scrutinize with a critical eye.

A key ingredient in permitting informed but relatively nonpartisan participation by parliamentarians is a strong committee support base, in terms of research and expert advice. The record of adequate support for parliamentary committees in Canada is not good, comparing unfavourably with the relatively more lavish resources accorded congressional committees in the US. A case could certainly be made for exceptional support for a national security committee, given its unusual challenges. But there is another, more attractive alternative to consider: providing external security-cleared expert advice to the committee on a continuing basis.[100]

It is here that we envisage a potentially useful relationship between the external, arm's-length review bodies and a parliamentary committee. The development of experienced, expert personnel in the review bodies – already evident for many years in SIRC – could be tapped by a parliamentary committee to assist in reviews for efficacy. The strengthened RCMP review body, the CSE commissioner and the enhanced SIRC, as recommended in the Arar Commission policy review, could offer a pool of expertise for the parliamentarians. The Integrated National Security Review Coordinating Committee recommended by O'Connor (made up of the heads of the review bodies and an independent chair) could do double duty as the coordinating body and main contact point between the parliamentary committee and the review bodies. This relationship of course presumes the provision of adequate resources to the review bodies so that they are enabled to perform their regular functions as well as to serve the parliamentary committee when required.

An advantage of this arrangement would be to encourage a more cooperative and complementary relationship between parliamentary and external review than has been evident at times in the past, the worst example of a breakdown in relations being the hostile relations that developed between SIRC and the parliamentary subcommittee on national security during the "Heritage Front" affair.

The McDonald Commission had envisioned complementary roles for Parliament and the permanent review body for CSIS. In this regard, it is important to recognize that legislative committees may not prove to be particularly good at performing certain types of scrutiny. American research suggests, in fact, that they may be good at what McGubbins and Schwartz have referred to as dealing with "fire alarms" but poor at doing the "police patrolling" form of scrutiny (McGubbins and Schwartz 1984; Born, Johnson, and Leigh 2005). However, given the fact that the capacity and potential performance dimensions of efficacy demand before-the-fact assessments if intelligence failures are to be limited, leaving matters entirely to legislative committees may not necessarily lead to positive outcomes. In other words, it is probably a mistake to divide accountability into watertight compartments. Even if Parliament concentrates its attention mainly on efficacy questions, some aspects of efficacy may still be left to the external review bodies (SIRC has for some years carried out some of the "police patrolling" scrutiny of CSIS).

One objection to this relationship might be that accountability for propriety, especially the adjudication of complaints against security agencies, requires a degree of quasi-judicial independence that efficacy investigations requiring some degree of before-the-fact assessments may call into question. In our view, there is no reason why the review bodies cannot compartmentalize themselves so as to assure sufficient impartiality on the part of those assessing complaints. On the other hand, SIRC has indicated that it would not wish to see its complaints function hived off because it has found that the investigation of complaints informs SIRC's understanding of how CSIS operates, thus improving its capacity to review for efficacy.

Another objection, and one that should be taken seriously, is that reform may result in too much review, impeding the agencies' capacity to carry out their normal functions and protect Canada's national security. While this argument has been used as a handy rationale by some for avoiding genuine oversight, this is a real risk, and we have already noted some instances of perverse effects of imposing greater accountability. Certainly any interference by external reviewers in ongoing operations would be counterproductive, but this practice is not part of existing reviews (SIRC, for instance, avoids investigating ongoing CSIS operations), nor should it be contemplated in any of the proposed new forms of review. While review for efficacy may include some before-the-fact knowledge of what is being done, this in no way implies any hands-on involvement

by reviewers in operational matters. Another concern of operational personnel is that expectation of *ex post facto* judgments by reviewers demanding adherence to unrealistic standards of behaviour may have the effect of making front-line people risk-averse and overly cautious ("better safe than sorry"), to the detriment of innovative responses to security threats. Much depends on how review is actually carried out, but even more on applying realistic and reasonable standards for both propriety and efficacy.

One way of allaying these fears is to address the key question of what we want accountability to do. Accountability for control can be left mainly to the executive, as can discipline and sanctions against individual employees for misbehaviour or incompetence, always a matter for internal systems of administrative control. External reviewers should focus on systemic and structural issues rather than individual behaviour. Accountability for learning can be a positive asset to any organization. External reviewers can point to mistakes made not as a way to punish individuals – though they may legitimately follow up to establish whether those responsible for the organization have properly dealt with such matters – but as a guide to how the organization can improve its performance and get better results. They can also usefully warn of potential pitfalls down the road that if left unaddressed may later have a damaging impact on the organization. It is interesting to note that, despite some rocky times early in the relationship between CSIS and SIRC, CSIS today readily acknowledges that on balance SIRC has made it a better organization than it would have been in the absence of an external review body, that it has in effect internalized many of the lessons of accountability, to its organizational benefit.[101]

Accountability for learning is closely related to accountability for assurance. In some ways the greatest net benefit to national security agencies of improved accountability is public legitimacy. One only has to look at the public relations difficulties that have befallen the RCMP in recent years, on both the national security and the law enforcement sides, in relation to its ineffective or dysfunctional external review procedures, to realize the potential value to the force itself of effective external review. Effective review, however, must mean real accountability, not pro forma whitewashes that leave the public unsatisfied, suspicious and resentful. Only effective review can offer genuine assurance to the public.

Review must of course be seen to be effective. In the case of national security matters, this presents special problems. Since national security agencies operate under heavy secrecy, and since those bodies carrying out reviews must operate under the same levels of secrecy, critics may remain skeptical of heavily censored or redacted reviews of secret operations, or even see cover-ups on the basis of relatively innocuous declassified parts of largely nondisclosable reports. In part, this difficulty is unavoidable. Ironically, in this context the best indicator of assurance may come when the review body has established a track record of public criticism of the agency it is reviewing (here the history of CSIS-SIRC relations is instructive).

There is another dimension here that should be addressed, and that is the overreliance on secrecy of the federal government. The history of the Arar Commission's protracted battles with Ottawa over the public disclosure of information provides a useful guide (Whitaker 2008, 11-5). This confrontation had the political effect of enhancing the legitimacy of the inquiry, while raising public suspicions of the government's motives. In the end, the dispute was settled in the Federal Court after the publication of the final report with additional material ordered disclosed. The additional material in no way risked national security but demonstrated that the government had fought to withhold some information that was potentially embarrassing, as well as some references that were patently innocuous although deemed nondisclosable according to technically strict and narrow interpretation. The lesson to be drawn is that if accountability in national security is to be effective, and seen to be effective, the government should steel itself to take a more expansive interpretation of what may be publicly disclosed in the course of reporting external review. Of course, genuine national security confidentiality must be strictly observed (it is notable that not a single instance of disclosure damaging to national security has ever been attributed to SIRC in its quarter-century of existence). But if improved accountability and public assurance are to be achieved, more reasonable flexibility in disclosure is essential.

Notes

1 The authors would like to thank Peter Gill, Loch Johnson, Philip Rosen and Thorsten Wetzling and the Institute for Research on Public Policy's anonymous reviewers for their comments.

2 See, for example, Canadian Institute of International Affairs (2004-05) and Charters (2008); Forcese (2008a); Roach (2007); Whitaker (2008).

3 *Federal Accountability Act*, S.C. 2006, chap. 9. Two important elements, however, were the designation of deputy ministers and the deputy heads of certain organizations as accounting officers and the appointment of a parliamentary budget officer. The accounting officers will likely extend the information that Parliament receives about the functioning of departments and agencies; the parliamentary budget officer will likely provide greater clarity to the budgetary process.

4 Controls over the appointment of political staffers to permanent public service positions, changes in the governance structure of the Canadian Dairy Commission and lower limits on campaign donations by individuals may be admirable initiatives in themselves, but are problematic components of enhanced administrative accountability.

5 Donald Savoie (2008a) argues: "The chain of accountability, from voters to MP, from MP to prime minister and cabinet ministers, from ministers to the heads of government departments and agencies, and from senior civil servants to front-line managers to their employees, has broken down...We should no longer tolerate court government, by which a political leader with the help of a handful of courtiers shapes and reshapes instruments of power at will." There are several important studies on the accountability roles of major institutions of government in the Gomery Commission's research.

6 As one well-informed commentator (Simpson 2007) has written on the perverse impact of the attempts to counter the sponsorship scandal: "New mini-bureaucracies, more paperwork, fresh regulations and over-the-top requirements to report who spoke to whom outside government are already having the perverse effect of making an already cumbersome government more cumbersome, and an already form- and procedure-driven bureaucracy even more bureaucratic. The effect of the Gomery inquiry, therefore, was to flush out shady characters and dubious, even illegal, actions but, over the long term, to make even less effective the operations of the federal government and less attractive that government as a place to work."

7 New measures also require internal auditing to be more independent. Treasury Board now requires deputy ministers to have a majority of external members on their departmental audit committees by April 2009 (Treasury Board 2008). The role of these committees is wide-ranging and in addition to the internal audit function encompasses financial and risk management, management controls, and values and ethics. See Treasury Board (2005).

8 Richard Ericson identified what he cleverly called "account ability" to describe "the capacity to provide a record of activities that explains them in a credible manner so that they appear to satisfy the rights and obligations of accountability" (1995, 137).

9 See Privy Council Office (2003).

10 Cabinet confidences are records designated by the Privy Council Office as belonging to the cabinet paper system. They include such documents as memoranda to cabinet, cabinet committee reports, records of decisions, agendas, aide-mémoires and documents prepared for cabinet committees.

11 The exclusion of classes of information from the Act is much more serious than exemption of information from disclosure. Exemptions may be appealed to the information commissioner and an injury test is applied. Exclusions cannot be appealed, and no tests may be applied.

12 *Canadian Security Intelligence Service Act*, R.S.C. 1985, chap. C-23 (CSIS Act), section 18 (1).

13 *Access to Information Act*, R.S.C. 1985, chap. A-1, sections 16(1)(c)(ii) and 17. Similar exemptions can be found in the *Privacy Act*, R.S.C. 1985, chap. P-21, sections 22(1)(b)(ii) and 25.

14 This was a major point of contention between CSIS and the RCMP in the investigation of the Air India bombing in 1985, once again reiterated in testimony before the Air India inquiry. It is a persistent source of tension between law enforcement agencies and intelligence agencies, the latter concerned not to endanger intelligence assets by exposure to public trials, and the former more concerned with securing criminal convictions.

15 *Canada Evidence Act*, R.S.C. 1985, chap. C-5.

16 *Anti-terrorism Act*, S.C. 2001, chap. 41, Part 3, sections 43-46.

17 US senator Daniel Moynihan, from his extensive experience in oversight of US intelligence, stressed: "Departments and agencies hoard information, and the government becomes a kind of market. Secrets become organizational assets, never to be shared save in exchange for another organization's assets...The system costs can be enormous. In the void created by absent or withheld information, decisions are either made poorly or not at all" (1998, 73).

18 A classic example of this concerned information about murders committed by Daniel Gingras and Allan Légère, who had escaped from separate federal prisons. Suspecting a cover-up, the Justice Committee demanded in 1991 to see a report by Corrections Canada. The Solicitor General offered only a copy released under the *Access to Information Act* on *Privacy Act* grounds. He finally released the full document when it became clear that the House would use its powers under Standing Order 108 (Farson 1996, 37-8).

19 One instance in which particular precautions were taken and where there could have been very significant consequences occurred when the Subcommittee on Organized Crime of the Standing Committee on Justice and Human Rights conducted its investigation in 1999-2000. Because

of threats received, the subcommittee decided to hold all of its proceedings in camera to protect witnesses, committee members and their staff. While the subcommittee was very careful to protect the confidentiality of sources and their evidence, even going to the point of identifying only recommendations in its report, one member of the subcommittee was severely chastised by the chair for releasing information to the media about the location of some of its hearings outside Ottawa.

20 *Security Offences Act*, R.S.C. 1985, chap. S-7.

21 For example, Standing Order 108, discussed later.

22 The questioning process has also recently become contentious. Justice John Gomery, for example, has recently criticized parliamentarians in this regard, suggesting that lawyers are more capable. Given that so many parliamentarians have legal training, this rationalization seems somewhat misconceived. Equally, criticism could be lodged against legal teams working for commissions of inquiry for not knowing what to ask. Perhaps some players are better at some forms of inquiry than others. Any evaluation of what is the best practice should take such matters into consideration and would need to encompass the politics of the matter, the time available, the resources at hand, etc.

23 Prime Minister Brian Mulroney made the apology in a statement in the House of Commons on September 22, 1988.

24 According to the 1971 census, the total population of Canada was 21,568,000: 800,000 files represent information on more than one out of every 27 Canadians. Even allowing for duplication, this represents a remarkable level of surveillance.

25 House of Commons, Debates, March 7, 1966, 2297.

26 It is unclear whether the government was following Mackenzie. According to John Starnes (1998, 131-3), he was initially asked if he was interested in being the first civilian commissioner of the RCMP.

27 This may partly be explained by the types of scandals involved. Loch K. Johnson has explored the distinction between low- and high-threshold scandals (2009).

28 A Quebec government inquiry, the Keable Commission (Commission d'enquête sur des opérations policières en territoire québécois), which reported in 1981, preceded the McDonald Commission described below.

29 Order-in-Council, PC 1977-1911, July 6, 1977.

30 On the political and bureaucratic background to civilianization see Littleton (1986, 135-62) and Whitaker (1991, 659-65).

31 A similar situation has more recently occurred in the US, where warrantless wiretaps in contravention of the *Foreign Intelligence Surveillance Act* were employed by the Bush administration. The experience reveals the limitations of both the internal and external oversight systems, as it was the media rather than Congress or the relevant inspector general (IG) that revealed this wrongdoing. In Canada, the CSEC was authorized by the *Anti-terrorism Act* to listen to communications involving Canadians when the origin of the call is from abroad. In all other circumstances, a warrant is required.

32 In theory, this means that the Parliament of Canada is not bound by such statutes as the *Privacy Act* or the *Access to Information Act* or such conventions as that covering *sub judice* matters. By comparison, New Zealand's *Intelligence and Security Act* 1996, which increased the level of "oversight and review," specifically binds the New Zealand Crown (section 4).

33 For example, the forerunners of the CSEC were established and moved between departments by executive order (Farson 2001, 78-94)

34 It might equally be noted that few MPs had fully grasped the powers and privileges available to them. This deficiency would subsequently be addressed by MP Derek Lee, a former member of the special committee that reviewed the *CSIS Act* and subsequently a chair of the Subcommittee on National Security, in the 1990s (1999). The *sub judice* convention holds that members of Parliament should not bring up matters in debates, questions and motions that are awaiting adjudication in a court of law. To thwart answers, government ministers have sometimes dubiously claimed that this rule also applied to matters under investigation by the police.

35 One of the worst examples of bureaucrats being abused by a committee occurred during the Al-Mashat hearings in the early 1990s. Normal practices were not followed. For example, Library of Parliament staff normally draw up a list of questions that witnesses might properly be asked. In this instance, they were informed that their services were not required (Sutherland 1991, 573-603).

36 The chair was MP Blaine Thacker. Parliamentary committee staff pale by comparison to those of US congressional committees. Yet the special committee had four researchers, instead of one or two, which was then normal.

37 Conflict between Parliament and SIRC has been evident on at least two important occasions. The first was during the five-year review process (discussed below). The other occurred during the Heritage Front affair. For a critical examination of the review process see Whitaker (1996, 279-305). For a contrary view by the then executive director of SIRC, see Archdeacon (1996, 306-12). See also Farson (1996, 38-46).

38 Subsection 2(c) was amended by the *Anti-terrorism Act* in 2001 to add the words "religious or ideological" (section 89).

39 McDonald had made recommendations regarding federal-provincial cooperation that were more hortatory than institutional in nature, leaving them to political and administrative discretion; there are specific provisions in the *CSIS Act* referring to cooperative arrangements with the provinces, and provincial police forces, on specific matters (sections 13[2] and 17).

40 *Royal Canadian Mounted Police Act*, R.S.C. 1985, chap. R-10, Part VI.

41 The solicitor general's office was superseded by the position of minister of public safety during a major reorganization of government in 2004.

42 Disclosed versions of the IG certificates are now made available on the IG's public website: http://www.publicsafety.gc.ca/abt/wwa/igcsis/igcsis-en.asp. It should be noted that the provision of these annual certificates to SIRC has not always been timely: i.e., within SIRC's annual reporting period.

43 There is one article from the late 1980s devoted entirely to the role of the IG of CSIS (Ryan 1989). For a comparative perspective, however, see Wellar (1996/97).

44 In the early 1990s one IG objected to what she took to be unreasonable limitations on her access to CSIS records relating to ongoing investigations. The minister supported the CSIS director on this point, and this IG resigned her position after a relatively short tenure (Whitaker 1999, 139). The director of CSIS refused to meet with another IG for years (Bronskill 1999). After this IG resigned, the post remained open for over a year. At the same time, there were delays in replacing two SIRC members (Fife 1999).

45 Memorandum, Solicitor General to Director of CSIS, Oct. 30, 1989 (Solicitor General 1991, 14).

46 SIRC investigated the Atwal warrant and concluded incompetence rather than malice was the problem (SIRC 1988, 11).

47 See testimony of Jack Hooper to the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Public Hearing, June 22, 2004, pp. 458-73. http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.stenotran.com/commission/maherarar/2004-06-22%20volume%202.pdf

48 In 2007, the Supreme Court of Canada struck down the original provisions of this legislation governing security certificates in its decision on Charkaoui v. Canada (Minister of Citizenship and Immigration), 2007 S.C.C. 9. Hitherto, evidence introduced by the government could not be tested by lawyers acting for those named in certificates. This process was one that made Federal Court justices uneasy as it forced them to act as advocates as well as judges (Hugessen 2002, 381-6). Revisions to the legislation subsequently removed this duty by installing special advocates. Such lawyers have appropriate security clearances that enable them both to test government evidence and to appear in closed hearings where they can cross-examine government witnesses. At no point are they in a solicitor-client relationship. In fact, they are obliged not to share any information that they come across with either the persons named in the certificate or their lawyers.

49 Section 34(1) of the *CSIS Act* establishes the criteria regarding the composition of SIRC.

50 Privy councillors are appointed for life by the governor general on the advice of the prime minister as advisers to the Crown. Traditionally, cabinet ministers are made privy councillors. They each take an oath. In SIRC's case, its appointees are named privy councillors at the time of their appointment. Each member of SIRC is appointed for a five-year term during good behaviour, and is eligible to be reappointed for a term not exceeding five years. Each takes the privy councillor's oath, which includes the requirement to keep things learned in the capacity of a privy councillor secret, as well as the oath of secrecy that employees of CSIS take.

51 No one has been appointed to SIRC who has a past affiliation with the Bloc Québécois, although the leader of that party in the House has been consulted over the appointment of members from Quebec. It took six years following its first appearance as a recognized party for the Reform/Canadian Alliance (now part of the Conservative Party) to gain a representative on the committee. SIRC has, however, always had one member with past affiliations to the New Democratic Party. Some members of SIRC have been politically independent. For the first few years, a government party representative served as chair, but in 2005 a Liberal government appointed the former Progressive Conservative premier of Manitoba as chair.

52 Beyond cabinet confidences, there is an additional exception to SIRC's access. In 1988, SIRC entered into a "third party access protocol" with CSIS that potentially limits SIRC's access to CSIS documents containing information provided by third parties (foreign governments and organizations) if the latter withhold consent, although CSIS "will use its best efforts to obtain authority to disclose information provided by third parties when requested to do so by SIRC" (memorandum from chairman of SIRC to director of CSIS, May 25, 1988, with Annex of same date, disclosed under Access to Information request to SIRC, January 23, 1995). In the mid-1990s, SIRC publicly complained when a CSIS document it had sought was instead returned to its donor agency (SIRC 1996, 5-6).

53 A list of SIRC's reports can be found at http://www.sirc-csars.gc.ca/opbapb/lsrlse-eng.html.

54 For an overview of TARC, see testimony of Jack Hooper to the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Public Hearing, June 22, 2004, pp. 458-73. http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.stenotran.com/commission/maherarar/2004-06-2%20volume%202.pdf. TARC is chaired by the director of CSIS, and includes senior CSIS officers as well as representatives from the Department of Justice and Public Safety Canada.

55 Testimony of John Adams, Chief of CSE, and other officials in Standing Senate Committee on National Security and Defence, Proceedings, Issue 15 – Evidence, April 30, 2007.

56 There have, however, been allegations that Canadians have been involved. In addition to denying these strenuously, the Canadian government has expressed concern about "false-flag operations," especially where Canadian passports have been used (Thorne 2009).

57 Prior to an amendment of the *CSIS Act* in 2001, SIRC also conducted investigations and hearings with respect to sections 39 and 81 of the *Immigration Act* and

recommendations for deportation on security or criminal grounds. Matters may also be referred to SIRC by the Canadian Human Rights Commission pursuant to section 45 of the *Canadian Human Rights Act*, when a minister advises the commission that a complaint is related to national security: *CSIS Act*, section 38.

58 The number of complaints excludes those dealing with the application of the *Official Languages Act* in the CSIS workplace. Between 1985 and 1987 alone, SIRC received 2,256 complaints under the latter category.

59 SIRC (2005), section 46(2).

60 Canada (Minister of Employment and Immigration) v. Chiarelli, [1992] 1 S.C.R. 711.

61 Thomson v. Canada (Deputy Minister of Agriculture), [1992] 1 S.C.R. 385.

62 SIRC 1987, 33-40. The impetus for closing the branch also came from a special task force headed by a senior public servant (Osbaldeston 1987; Gill 1989).

63 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, Justice John Major, Commissioner.

64 The most acerbic journalistic critic has been Andrew Mitrovica, who writes about a "sort of Stockholm Syndrome within the intelligence community" in concluding that "SIRC, ironically is often CSIS's best friend." He adds that "the important and necessary business of watching over the watchers cannot be left to a handful of part-time, political appointees who are often preoccupied with their business interests, legal careers and other pursuits" (2002, 293, 332-3). There is a considerable literature on "co-optation": in the US, see Aberbach (1990), and for a comparative analysis see Born, Johnson, and Leigh (2005).

65 In 2005, a news report quoted SIRC as claiming that CSIS "purposefully misled" it and attempted to "suppress information that was embarrassing to the Service" (Curry and Freeze 2005). In its Annual Report 2005-2006, 12-14, SIRC took issue on a number of counts with the manner in which CSIS was handling exchanges of information on Canadians with countries with questionable human rights records, a highly contentious issue that has been the subject of both the Arar Commission and the Iacobucci Inquiry.

66 Laurence Lustgarten and Ian Leigh write that SIRC "has pushed CSIS into what was described as 'pre-emptive change'. That is, CSIS has done things it would probably not have done, sometimes in more radical fashion than SIRC itself might have suggested. The very existence of a review body pushed the Service into integrating into its own decision-making the kinds of considerations SIRC exists to voice publicly" (1994, 461). On the concept of an organizational culture in intelligence agencies, see Farson (1991a, 185-217).

67 One of the authors (Stuart Farson) served as director of research for the special committee.

68 Among the documents denied were the annual reports of the director, SIRC reports (except its annual reports), the IG's certificates, the service's policy and budgetary papers.

69 The special committee's record regarding its recommendations for statutory reform may not be as poor as is often assumed. A senior official with particular responsibilities for the two acts did suggest in a private conversation with one of the authors that many of the recommendations were taken up through policy initiatives.

70 As a subcommittee, its reports would have to be approved by the full standing committee.

71 For the use of such executive orders regarding CSEC prior to the adoption of its enabling statute in 2001, see Farson (2001, 78-94).

72 Its existence had first been identified as early as 1975 by the US publication *Ramparts* and subsequently by the CBC.

73 Privacy Commissioner (1996, 52); Auditor General of Canada (1996, chap. 27, main point 53).

74 Order-in-Council, PC 1996-899, June 19, 1996.

75 By May 2007, some 40 classified reports had been submitted (Communications Security Establishment Commissioner 2006, Annex B).

76 See, for example, Communications Security Establishment Commissioner (2002, 3-4).

77 Amendments to the *National Defence Act*, R.S.C. 1985, chapter N-5, section 273.63.

78 Ibid., 3.

79 Arguably, both of these functions are essential. Bill Robinson has shown that the CSEC failed at one point to keep up with technological developments (1992). Signals intelligence has changed dramatically as new communications technologies have come on stream. This means that law and accountability procedures must similarly keep up.

80 Communications Security Establishment Commissioner (2006, 13).

81 Although Commissioner Claude Bisson appeared during consideration of the *Anti-terrorism Act*, no commissioner testified before the Standing Committee on National Defence and Veterans Affairs on the office's annual reports before 2004. See Commissioner Antonio Lamer's evidence to that committee on April 20, 2004, at http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=1307211&Language=E&Mode=1&Parl=37&Ses=3.

82 Auditor General of Canada (1996). The US GAO has been routinely denied cooperation by the CIA, although recently the US Department of Defense has directed "explicitly for the first time that GAO requests for foreign intelligence and counterintelligence information may be granted" ("DOD Should Not 'Categorically' Deny GAO Access to Intelligence" 2009).

83 Auditor General of Canada 2003, 10.139.

84 Auditor General of Canada 2003, 10.154.

85 Auditor General of Canada 2003, 10.162.

86 Auditor General of Canada 2004.

87 Auditor General of Canada 2005.

88 This was until recently a classified document and is now available to the public only in redacted form.

89 One of the authors (Whitaker) was chair of the panel.

90 "Speaking Remarks by David Brown at the Release of the Report of the Task Force." December 14, 2007. http://www.publicsafety.gc.ca/rcmp-grc/sn-eng.aspx. Brown recommends a new Independent Commission for Complaints and Oversight for the RCMP, explicitly designed as an accountability mechanism for assurance and legitimation: "the goal [is] restoring and maintaining confidence of the public and the members and employees of the Force" (Task Force on Governance and Cultural Change in the RCMP, 17). See also House of Commons Standing Committee on Public Accounts (2007).

91 We have distinguished between a committee of parliamentarians and a parliamentary committee (Farson and Whitaker 2007).

92 One of the authors (Whitaker) was a member of a five-person panel advising O'Connor on the policy review, and thus participated in shaping the recommendations that are laid out here. The other (Farson) was an expert witness in this part of the inquiry.

93 Examples include the Integrated National Security Enforcement Teams (INSETs), which work together under RCMP direction but involve CSIS and other federal agencies, as well as provincial police forces where appropriate; and Integrated Border Enforcement Teams (IBETs) and other similar cooperative efforts that may involve not only federal and provincial agencies but American federal and state agencies as well. INSETs have registered one apparent success in the 2006 arrests of 18 alleged terrorists in Toronto, though charges have so far been stayed against several of those originally charged.

94 In personal conversation with the authors, the former chair, Shirley Heafey, described the complaints commission system as "broken."

95 The PCO is responsible not only for the development and coordination of community-wide security and intelligence policy, but also for the International Assessment Staff, both under the direction of the national security adviser. Presumably, the PCO was not considered because O'Connor was focusing on propriety issues. O'Connor did recommend that after five years, reconsideration should be given to whether other federal agencies should be subject to review. A recent example of expanding intelligence collection by the Canadian government with potential implications for accountability is a report that the Defence Department is developing a human intelligence gathering capacity for foreign deployments ("New Military Spy Unit to Gather Information on Overseas Missions" 2008).

96 One might equally argue that it was a fallacy to believe that disbanding the RCMP Security Service somehow also detached the RCMP from its counterterrorism responsibilities and the intelligence process that this work demanded (Farson 1991c).

97 For example, the policy side of the Arar Commission required O'Connor to make recommendations for "an independent arm's-length review mechanism for the RCMP" and to consider how the recommended mechanism would interact with "other review bodies." Arguably, he interpreted this mandate literally, and avoided any discussion of Parliament's involvement. One impact of this has been that the RCMP has responded only to his specific recommendations on the force, not to the broader question of how it might inform Parliament about national security criminal investigations.

98 Impropriety in the special case of national security should not be seen as limited to illegality, but may encompass actions that are technically legal within the special framework that applies to national security activities but may nonetheless be judged unethical or inappropriate according to the wider framework of social values. Thus, accountability for propriety has gone beyond the simple verification of the legality of the actions of national security officials to the interrogation of the legal framework within which they operate. This framework itself, as well as the resultant practices of the agencies, has undergone successive reforms over the years to reflect shortcomings revealed by outside scrutiny. Thus, the criteria established in the *CSIS Act* for what activities that agency can and cannot appropriately target for intrusive surveillance provided outside reviewers with sufficient reason to recommend successfully the closure of the Counter-Subversion Branch – not because that branch was operating illegally, but because it was targeting inappropriately in light of the principles enunciated in the Act. Similarly, the Arar Commission pointed to intelligence-sharing practices by the RCMP that had disastrous consequences for the human rights of Maher Arar; these practices were not illegal, but they were inappropriate, and thus subject to calls for reform on grounds of impropriety.

99 We have explored how other countries have adapted the committee of parliament option (Farson and Whitaker 2009).

100 With regard to parliamentary review of anti-terrorism legislation, Craig Forcese, drawing on the UK and Australian examples, makes a strong case for what he calls "precursor expert review" to inform parliamentary committees in Canada (2008a).

101 See the answer given by Ward Elcock, the longest-serving director of CSIS, regarding SIRC's influence: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Public Hearing, June 21, 2004, p. 187 (http://epe.lac-bac.gc.ca/100/206/301/pco-cp/commissions/maher_arar/07-09-13/www.stenotran.com/commission/maherarar/2004-06-21%20volume%201.pdf. accessed July 13, 2009).

References

Aberbach, Joel D. 1990. *Keeping a Watchful Eye: The Politics of Congressional Oversight.* Washington, DC: Brookings Institution.

Adachi, Ken. 1976. *The Enemy That Never Was: A History of Japanese Canadians.* Toronto: McClelland and Stewart.

Advisory Panel on the Review of the CATSA Act. 2006. *Flight Plan: Managing the Risks in Aviation Security.* Ottawa: CATSA Act Review Secretariat.

Akkad, Omar El. 2008. "Proposed Army Spy Unit Raises Worry: Critics Suspicious of Operations 'Unknown to Canadians.'" *Globe and Mail,* May 27.

Archdeacon, Maurice. 1996. "The Heritage Front Affair." *Intelligence and National Security* 11 (2).

Aucoin, Peter, and Heintzman, Ralph. 2000. "The Dialectics of Accountability for Performance in Public Management Reform." *International Review of Administrative Sciences* 66 (1).

Auditor General of Canada. 1996. "The Canadian Intelligence Community: Control and Accountability." In *1996 November Report of the Auditor General of Canada.* Ottawa: Office of the Auditor General.

———. 2003. *2003 November Report of the Auditor General of Canada.* Ottawa: Office of the Auditor General.

———. 2004. "National Security in Canada: The 2001 Anti-terrorism Initiative." In *2004 March Report of the Auditor General.* Ottawa: Office of the Auditor General.

———. 2005. *2005 April Report of the Auditor General of Canada.* Ottawa: Office of the Auditor General. Accessed July 13, 2009. http://www.oag-bvg.gc.ca/internet/English/parl_oag_200504_e_1120.html

Born, Hans, Loch K. Johnson, and Ian Leigh. 2005. *Who's Watching the Spies? Establishing Intelligence Service Accountability.* Washington, DC: Potomac Books.

Bronskill, Jim. 1999. "The Spy Who Snubbed Me: Watchdog Says CSIS Boss Refused Meetings for Years." *Gazette,* June 3.

Campbell, Anthony. 2009. "Bedmates or Sparring Partners? Canadian Perspectives on the Media-Intelligence Relationship in the 'New Propaganda Age.'" In *Known Knowns: Why Intelligence Needs the Media, Why the Media Needs Intelligence,* edited by R. Dover and M.S. Goodman. London: Hurst.

Canadian Institute of International Affairs. 2004-05. "Security in an Age of Terrorism." Special issue, *International Journal* 60 (1).

Charters, David A. 2008. "The Un)Peaceable Kingdom? Terrorism and Canada before 9/11." *IRPP Policy Matters* 9 (4).

Clark, Campbell. 2005. "Late in the Day for a Public Inquiry." *Globe and Mail,* March 17.

———. 2007. "RCMP 'Horribly Broken,' Investigator Finds." *Globe and Mail,* June 15.

Cleroux, Richard. 1990. *Official Secrets.* Scarborough, ON: McGraw-Hill Ryerson.

Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. 1981. *Freedom and Security under the Law: Second Report.* 2 vols. David C. McDonald, chair. Ottawa: the Commission.

Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. 2004. "Deputy Prime Minister Issues Terms of Reference for the Public Inquiry into the Maher Arar Matter." Accessed July 13, 2009. http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/Terms_of_Reference.pdf

———. 2006a. *A New Review Mechanism for the RCMP's National Security Activities.* Dennis R. O'Connor, Commissioner. Ottawa: Public Works and Government Services Canada.

———. 2006b. *Report of the Events Relating to Maher Arar.* 3 volumes. Dennis R. O'Connor, Commissioner. Ottawa: Public Works and Government Services Canada.

Commission of Inquiry into the Deployment of Canadian Forces to Somalia. 1997. *Dishonoured Legacy: The Lessons of the Somalia Affair.* Gilles Létourneau, commissioner. 5 volumes. Ottawa: Canadian Government Publishing.

Communications Security Establishment Commissioner. 2002. *Annual Report 2001-2002.* Ottawa: Office of the Commissioner.

———. 2006. *Annual Report 2005-2006.* Ottawa: Office of the Commissioner.

Cooper, Barry. 2007. *CFIS: A Foreign Intelligence Service for Canada.* Calgary: Canadian Defence & Foreign Affairs Institute.

Curry, Bill, and Colin Freeze. 2005."CSIS 'Misled' Watchdog: Secret Report Blasts Agency's Investigation of Public Servant It Deemed a Security Risk." *Globe and Mail,* September 14.

Davies, Marc. 2002. "Guarding the Guardians." PhD thesis. University of Wales at Aberystwyth.

"DOD Should Not 'Categorically' Deny GAO Access to Intelligence." 2009. *Secrecy News* (FAS Project on Government Secrecy) 2009, no. 12, February 4.

Edwards, J. Ll. J. 1980. *Ministerial Responsibility for National Security as It Relates to the Offices of Prime Minister, Attorney General and Solicitor General of Canada.* Study prepared for the McDonald Commission. Ottawa: Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police.

Ericson, Richard V. 1995. "The News Media and Account Ability in Criminal Justice." In *Accountability for Criminal Justice: Selected Essays,* edited by Philip C. Stenning. Toronto: University of Toronto Press.

Farson, Stuart. 1991a. "Old Wine, New Bottles and Fancy Labels: The Rediscovery of Organizational Culture in the Control of Intelligence." In *Crimes by the Capitalist State: An Introduction to State Criminality,* edited by Greg Barak. New York: State University of New York Press.

———. 1991b. "Restructuring Control in Canada: The McDonald Commission of Inquiry and Its Legacy." In *Controlling Intelligence,* edited by Glen Hastedt. London: Frank Cass.

———. 1991c. "Security Intelligence Versus Criminal Intelligence: Lines of Demarcation, Areas of Obfuscation and the Need to Re-evaluate Organizational Roles in Responding to Terrorism." *Policing and Society* 2 (1): 65-87.

———. 1995. "'The Noble Lie' Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability?" In *Accountability for Criminal Justice: Selected Essays*, edited by Philip C. Stenning. Toronto: University of Toronto Press

———. 1996. "In Crisis and in Flux? Politics, Parliament and Canada's Intelligence Policy." *Journal of Conflict Studies* 16 (1).

———. 2000. "Parliament and Its Servants: Their Role in Scrutinizing Canadian Intelligence." *Intelligence and National Security* 15 (2).

———. 2001. "So You Don't Like Our Cover Story – Well We Have Others: The Development of Canada's Signals Intelligence Capacity through Administrative Sleight of Hand, 1941-2000." In *(Ab)Using Power: The Canadian Experience*, edited by Bob Menzies, Dorothy Chunn, and Susan Boyd. Halifax: Fernwood Press.

Farson, Stuart, and Reg Whitaker. 2007. "Democratic Deficit Be Damned: The Executive Use of Legislators to Scrutinize National Security in Canada." In *Understanding the Hidden Side of Government*. Volume 1 of *Strategic Intelligence*, edited by Loch K. Johnson, 65-88. Westport, CT: Praeger Security International.

———. 2008. "Canada." In *The Americas and Asia*. Volume 1 of *PSI Handbook of Global Security and Intelligence*, edited by Stuart Farson, Peter Gill, Mark Phythian, and Shlomo Shpiro, 21-51. Westport, CT: Praeger Security International.

———. 2009. "Accounting for the Future or the Past? Developing Accountability and Oversight Systems to Meet Future Intelligence Needs." In *Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson. New York: Oxford University Press.

Fife, Robert. 1999. "Lack of Supervision at Spy Agency Lamented: Watchdog Post Vacant." *National Post*, May 28.

Forcese, Craig. 2006. "Through a Glass Darkly: The Role and Review of 'National Security' Concepts in Canadian Law." *Alberta Law Review* 43 (4).

———. 2008a. "Fixing the Deficiencies in Parliamentary Review of Anti-terrorism Law: Lessons from the United Kingdom and Australia." *IRPP Choices* 14 (6). Montreal: IRPP.

———. 2008b. *National Security Law: Canadian Practice in International Perspectives*. Toronto: Irwin Law.

Franks, C.E.S. 1980. *Parliament and Security Matters*, Study Prepared for the McDonald Commission. Ottawa: Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police.

Freeze, Colin. 2006. "Spy Chief Reveals Extent of Foreign Missions." *Globe and Mail*, October 28.

———. 2008. "Rules Urged for Spies in Afghanistan." *Globe and Mail*, May 9.

Gill, Peter. 1989. "Symbolic or Real? The Impact of the Canadian Security Intelligence Review Committee, 1984-1988." *Intelligence and National Security* 4 (3): 550-75.

———. 2007. "Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the 'War on Terror.' *Intelligence and National Security* 22 (1): 14-37.

Glees, Anthony, Philip H.J. Davies, and John L. Morrison. 2006. *The Open Side of Secrecy: Britain's Intelligence and Security Committee*. London: Social Affairs Unit.

Good, David A. 2003. *The Politics of Public Management: The HRDC Audit of Grants and Contributions*. Toronto: University of Toronto Press.

Hennessy, Peter. 1990. *Whitehall*. London: Fontana Press.

House of Commons Special Committee on the Review of the *Canadian Security Intelligence Act* and the *Security Offences Act*. 1990. *In Flux but Not in Crisis*. Ottawa: Supply and Services Canada.

House of Commons Standing Committee on Public Accounts. 2007. *Restoring the Honour of the RCMP: Addressing Problems in the Administration of the RCMP's Pension and Insurance Plans*. Ottawa: the Committee.

Hugessen, James K. 2002. "Watching the Watchers: Democratic Oversight." In *Terrorism, Law and Democracy: How is Canada Changing following September 11?* edited by David Daubney, Wade Deisman, Daniel Jutras, Errol P. Mendes, and Patrick A. Molinari. Montreal: Les Éditions Thémis.

Independent Advisory Team on the Canadian Security Intelligence Service. 1987. *People and Process in Transition: Report to the Solicitor General*. Gordon Osbaldeston, chair. Ottawa: Solicitor General Canada.

Independent Panel on Canada's Future Role in Afghanistan. Report. 2008. John Manley, chair. Ottawa: Minister of Public Works and Government Services. Accessed April 25, 2009. http://dsp-psd.tpsgc.gc.ca/collection_2008/dfait-maeci/FR5-20-1-2008E.pdf

Johnson, Loch K. 2005. "Governing in the Absence of Angels: On the Practice of Intelligence Accountability in the United States." In *Who's Watching the Spies? Establishing Intelligence Service Accountability*, edited by Hans Born, Loch K. Johnston, and Ian Leigh. Washington, DC: Potomac Books.

———. 2008. "The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability." *Intelligence and National Security* 23 (2): 198-225.

———. 2009. "A Shock Theory of Congressional Accountability for Intelligence." In *Handbook of Intelligence Studies*. London: Routledge.

Knight, Amy. 2005. *How the Cold War Began: The Gouzenko Affair and the Hunt for Soviet Spies*. Toronto: McClelland and Stewart.

Lee, Derek. 1999. *The Powers of Parliamentary Houses to Send for Persons, Papers & Records: A Sourcebook on the Law and Precedent of Parliamentary Subpoena Powers for Canadian and Other Houses*. Toronto: University of Toronto Press.

Leigh, Ian. 1996. "Secret Proceedings in Canada." *Osgoode Hall Law Journal* 34 (1).

Light, Paul C. 1993. *Monitoring Government: Inspectors General and the Search for Accountability*. Washington, DC: Brookings Institution.

Littleton, James. 1986. *Target Nation: Canada and the Western Intelligence Network*. Toronto: Lester & Orpen Dennys.

Lustgarten, Laurence, and Ian Leigh. 1994. *In from the Cold: National Security and Parliamentary Democracy.* Oxford: Oxford University Press.

Marshall, Geoffrey. 1978. "Police Accountability Revisited." In *Policy and Politics*, edited by D. Butler and A. Halsey. London: Macmillan.

McGubbins, Mathew, and Thomas Schwartz. 1984. "Congressional Oversight Overlooked: Police Patrols versus Fire Alarms." *American Journal of Political Science* 28 (1): 165–79.

Mitrovica, Andrew. 2002. *Covert Entry: Spies, Lies and Crimes inside Canada's Secret Service.* Toronto: Random House Canada.

Moynihan, Daniel Patrick. 1998. *Secrecy: The American Experience.* New Haven and London: Yale University Press.

National Commission on Terrorist Attacks upon the United States. 2004. *The 9/11 Commission Report.* New York: W.W. Norton.

"New Case of Afghan Prisoner Abuse: Canadian Officials." 2007. *Toronto Star*, November 14.

"New Military Spy Unit to Gather Information on Overseas Missions." 2008. CBC News, May 26.

Osbaldeston, Gordon F. 1987. *People and Process in Transition.* Report to the Solicitor General by the Independent Advisory Team on the Canadian Security Intelligence Service. Published under the authority of the Hon. James Kelleher, Solicitor General of Canada. October.

Phythian, Mark. 2007. "The British Experience with Intelligence Accountability." In *Intelligence and Accountability: Safeguards against the Abuse of Secret Power.* Volume 5 of *Strategic Intelligence*, edited by Loch K. Johnson, 67–88. Westport, CT: Praeger Security International.

Privacy Commissioner. 1996. *Annual Report 1995–96.* Ottawa: the Commissioner.

Privy Council Office. 2003. *Guidance for Deputy Ministers.* Ottawa: PCO. Accessed April 27, 2009. http://www.pco-bcp.gc.ca/index.asp?lang=eng&page=information&sub=publications&doc=gdm-gsm/doc-eng.htm

Public Safety Canada. 2004. "A National Security Committee of Parliamentarians." Ottawa: Public Safety Canada. Accessed July 16, 2009. http://ww2.ps-sp.gc.ca/publications/national_security/nat_sec_cmte_e.asp

Rankin, Murray. 1990. "The Security Intelligence Review Committee: Reconciling National Security with Procedural Fairness." *Canadian Journal of Administrative Law and Practice* 3 (2): 173–97.

Roach, Kent. 2007. "Better Late Than Never? The Canadian Parliamentary Review of the *Anti-terrorism Act*." *IRPP Choices* 13 (5). Montreal: IRPP.

Robinson, Bill. 1992. "The Rise and Fall of Cryptanalysis in Canada." *Cryptologia* 16 (1): 23–38.

Rosen, Philip. 1993. "The Communications Security Establishment: Canada's Most Secret Intelligence Agency." Background Paper BP-343E. Ottawa: Library of Parliament, Parliamentary Research Branch.

Royal Commission on Security. 1969. *Report (Abridged).* M.W. Mackenzie, chair. Ottawa: Queen's Printer.

Royal Commission to Investigate the Communication of Secret and Confidential Information to Agents of a Foreign Power. 1946. *Report.* Robert Taschereau and R. L. Kellock, commissioners. Ottawa: King's Printer.

Ryan, Joseph. 1989. "The Inspector General of the Canadian Security Intelligence Service." *Conflict Quarterly* 9 (2): 33–51.

Sallot, Jeff. 2005. "Mounties Thwarting Complaints Process, Watchdog Says: RCMP Often Ignore Her, Chairwoman Adds." *Globe and Mail*, March 2.

Saltstone, Scot P. 1991. "Some Consequences of the Failure to Define the Phrase 'National Security.'" *Conflict Quarterly* 11 (3): 36–54.

Savoie, Donald J. 2003. *Breaking the Bargain: Public Servants, Ministers, and Parliament*, Toronto: University of Toronto Press

———. 2008a. "The Broken Chain of Answerability." *Globe and Mail*, May 16.

———. 2008b. *Court Government and the Collapse of Accountability in Canada and the United Kingdom.* Toronto: University of Toronto Press.

Schedler, Andreas. 1999. "Conceptualizing Accountability." In *The Self-Restraining State: Power and Accountability in New Democracies*, edited by Andreas Schedler, Larry Diamond, and Marc F. Plattner. London: Lynne Rienner Publishers.

Seaborn, Blair. 1985. "Report on Security Arrangements Affecting Airports and Airlines in Canada." Prepared for the Privy Council Office, Interdepartmental Committee on Security and Intelligence.

Security Intelligence Review Committee (SIRC). 1987. *Annual Report 1986–1987.* Ottawa: SIRC.

———. 1988. *Annual Report 1987–1988.* Ottawa: SIRC.

———. 1989. *Amending the CSIS Act: Proposals for the Special Committee of the House of Commons.* Ottawa: SIRC.

———. 1994. *The Heritage Front Affair: Report to the Solicitor General.* Ottawa: SIRC.

———. 1996. *Annual Report 1995–1996.* Ottawa: SIRC.

———. 1998. *Annual Report 1997–1998.* Ottawa: SIRC.

———. 2002. *Annual Report 2001–2002.* Ottawa: SIRC.

———. 2003. *Annual Report 2002–2003.* Ottawa: SIRC.

———. 2005. *Rules of Procedure.* Ottawa: SIRC. Accessed April 27, 2009. http://www.csars-sirc.gc.ca/cmpplt/rul-reg-eng.html

———. 2006. *Annual Report 2005–2006.* Ottawa: SIRC.

Senate Special Committee on the Canadian Security Intelligence Service. 1983. *Delicate Balance: A Security Intelligence Service in a Democratic Society.* Michael Pitfield, chair. Ottawa: the Committee.

Shephard, Michelle. 2005. "Mountie Secrets Hinder Rights Monitor: Arar Inquiry Gets Damning Report." *Toronto Star*, March 2.

Simpson, Jeffrey. 2007. "If Previous Inquiries Are Any Guide, Perverse Fallout Is A-comin." *Globe and Mail*, November 16.

Solicitor General. 1991. *On Course: National Security for the 1990s.* Ottawa: Supply and Services Canada.

Starnes, John. 1998. *Closely Guarded: A Life in Canadian*

Security and Intelligence. Toronto: University of Toronto Press

Sutherland, Sharon. 1991. "The Al-Mashat Affair: Administrative Accountability in Parliamentary Institutions." *Canadian Public Administration* 34 (4).

Task Force on Governance and Cultural Change in the RCMP. 2007. *Rebuilding the Trust*. Ottawa: Government of Canada.

Thorne, Stephen. 2009. "Ottawa Denies Knowledge of 'Sarah the Canadian.'" *Globe and Mail*, February 6.

Treasury Board. 2005. *Directive on Departmental Audit Committees*. Ottawa: Treasury Board Secretariat. Accessed April 27, 2009. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12342&section=text

———. 2008. *General Information on the Appointment of Department and Agency Audit Committee (DAAC) Members*. Ottawa: Treasury Board Secretariat. Accessed April 27, 2009. http://www.tbs-sct.gc.ca/iac-cvi/docs/general-generaux-eng.asp

Weber, Max. 1970. *From Max Weber: Essays in Sociology*, edited by H.A. Gerth and C. Wright Mills. London: Routledge.

Wellar, Geoffrey. 1996/97. "Comparing Western Inspectors General of Security and Intelligence." *International Journal of Intelligence and CounterIntelligence* 9 (4): 383–406.

Whitaker, Reg. 1991. "The Politics of Security Intelligence Policy-making in Canada: 1, 1970-84." *Intelligence and National Security* 6 (4): 649–68.

———. 1996. "The 'Bristow Affair': A Crisis of Accountability in Canadian Security Intelligence." *Intelligence and National Security* 11 (2): 279–305.

———. 1999. "Designing a Balance between Freedom and Security." In *Ideas in Action: Essays on Politics and Law in Honour of Peter Russell*, edited by Joseph F. Fletcher. Toronto: University of Toronto Press.

———. 2008. "Arar: The Affair, the Inquiry, the Aftermath." *IRPP Policy Matters* 9 (1). Montreal: IRPP.

Whitaker, Reg, and Gary Marcuse. 1994. *Cold War Canada: The Making of a National Insecurity State, 1945–1957*. Toronto: University of Toronto Press

Publications

Security and Democracy/ Securité et démocratie

"Canada's National Security 'Complex': Assessing the Secrecy Rules"
Craig Forcese
IRPP Choices, Vol. 15, no. 5 (June 2009)

"The (Un)Peaceable Kingdom? Terrorism and Canada before 9/11"
David Charters
IRPP Policy Matters, Vol. 9, no. 4 (October 2008)

"Fixing the Deficiencies in Parliamentary Review of Anti-terrorism Law: Lessons from the United Kingdom and Australia"
Craig Forcese
IRPP Choices, Vol. 14, no. 6 (May 2008)

"Better Late than Never? The Canadian Parliamentary Review of the *Anti-terrorism Act*"
Kent Roach
IRPP Choices, Vol. 13, no. 5 (September 2007)

National Security and Interoperability/ Sécurité nationale et l'intéroperabilité

"Weak States and Sudden Disasters and Conflicts: The Challenge for Military/NGO Relations"
Various authors
Conference paper, June 2005

Geopolitical Integrity
Hugh Segal (ed.)
Monograph, April 2005

"Mature Peacekeeping Operations as Facilitators of Organized Crime"
Irv Marucelj
Working paper 2005-1 (March 2005)

"Guarding the Continental Coasts: United States Maritime Homeland Security and Canada"
Joel J. Sokolsky
Policy Matters, Vol. 6, no. 1 (March 2005)

"Happiness Is – a Rising Defence Budget?"
Don Macnamara
Special report (February 2005)

"Canadian Naval Future: A Necessary Long-Term Planning Framework"
Peter Haydon
Working paper 2004-12 (November 2004)

"Addressing the Security-Development Nexus: Implications for Joined-up Government"
Ann M. Fitz-Gerald
Policy Matters, Vol. 5, no. 5 (July 2004)

"Realism Canadian Style: The Chrétien Legacy in National Security Policy"
Joel J. Sokolsky
Policy Matters, Vol. 5, no. 2 (June 2004)

"Force Structure or Forced Structure? The 1994 White Paper on Defence and the Canadian Forces in the 1990s"
Sean M. Maloney
Choices, Vol. 10, no. 5 (May 2004)

"A Vigilant Parliament: Building Competence for Effective Parliamentary Oversight"
Douglas L. Bland, Roy Rempel
Policy Matters, Vol. 5, no. 1 (February 2004)

"Four US Military Commands: NORTHCOM, NORAD, SPACECOM, STRATCOM – The Canadian Opportunity"
Joseph T. Jockel
Working paper 2003-3 (November 2003)

"Are We Just Peacekeepers? The Perception Versus the Reality of Canadian Involvement in the Iraq War"
Sean M. Maloney
Working paper 2003-2 (November 2003)

"The SORT Debate: Implications for Canada"
Philippe Lagassé
Working paper 2003-1 (October 2003)

"Military and Postconflict Security: Implications for American, British and other Allied Force Planning and for Postconflict Iraq"
Ann M. Fitz-Gerald
Choices, Vol. 9, no. 3 (April 2003)

IRPP

Accountability in and for National Security

Reg Whitaker and Stuart Farson

Résumé

Reg Whitaker et Stuart Farson examinent dans cette étude le système d'imputabilité qui s'applique aux agences et ministères gouvernementaux chargés de la sécurité nationale du Canada, puis ils formulent des recommandations visant à le réformer.

Chacun s'entend aujourd'hui pour accroître l'imputabilité gouvernementale, mais sans nécessairement en comprendre tous les enjeux. La notion d'imputabilité exige en effet une analyse approfondie, et ses objectifs doivent être clairement définis, car la volonté d'accroître le niveau d'imputabilité a trop souvent produit des résultats imprévus par le passé, voire certains effets indésirables. La sécurité nationale soulève à cet égard des défis particuliers, par ses exigences exceptionnelles en matière de secret notamment et aussi en raison du rapport complexe entre les activités de renseignement et l'application de la loi.

Pour analyser la notion d'imputabilité dans le domaine de la sécurité nationale, les auteurs portent une attention particulière aux concepts d'« examen » et de « surveillance ». Souvent perçu comme une mesure post facto, l'examen est généralement considéré au Canada comme l'option privilégiée pour accroître l'imputabilité. Mais les auteurs s'interrogent sur la pertinence de ce choix dans le domaine examiné. Ils montrent que les mécanismes d'imputabilité ont surtout eu pour fin de vérifier le bien-fondé et l'efficacité des programmes, deux critères interdépendants mais différents. Si l'examen semble adapté au premier critère, la surveillance paraît plus appropriée lorsqu'on vise l'efficacité. Les auteurs préconisent donc d'élargir notre conception de l'imputabilité en prenant en considération tant l'examen que la surveillance. Ils proposent aussi d'établir une nette distinction entre l'imputabilité *au sein* du ministère responsable de la sécurité nationale (c'est-à-dire au niveau de l'autorité exécutive et principalement pour des raisons de contrôle) et *aux fins* de la sécurité nationale (c'est-à-dire l'obligation de rendre compte des ministres répondant de l'action gouvernementale devant le Parlement).

L'étude retrace l'historique des mécanismes d'imputabilité au Canada en expliquant comment, quand et pourquoi on les a adoptés. Généralement suscitées par un scandale public, les réformes en ce domaine ont surtout visé à vérifier le bien-fondé. Mais depuis le 11 septembre 2001, de nouvelles formes de menaces à la sécurité ont soulevé de nouveaux défis. Les processus d'imputabilité doivent donc s'adapter aux réalités actuelles en intégrant les deux aspects du bien-fondé et de l'efficacité. La recherche d'une plus grande imputabilité a certes connu des avancées, mais le processus n'est pas encore terminé, observent les auteurs.

Dans le débat sur les meilleurs moyens de scruter les activités des milieux du renseignement et de la sécurité, on n'a toujours pas déterminé clairement ce que doivent accomplir les différents organismes et processus. L'enjeu clé réside ici dans l'étendue des pouvoirs disponibles et la meilleure manière de les exercer. Trois éléments revêtent une importance capitale : l'accès aux personnes et aux documents ; le pouvoir d'exiger des réponses précises et complètes ; le processus, la synchronisation, la substance et l'indépendance de la procédure de reddition de compte.

Les recommandations des auteurs sont de deux ordres. Compte tenu de l'intégration croissante des opérations de sécurité nationale gouvernementales et intergouvernementales, ils recommandent premièrement que les mécanismes d'imputabilité débordent des frontières institutionnelles. Deuxièmement, ils recommandent que le rôle du Parlement dans le processus d'imputabilité soit renforcé, en étroite coordination avec les organismes d'examen et de surveillance existants. Mais, avertissent-ils en terminant, cette imputabilité accrue ne doit aucunement entraver les activités de ceux qui protègent la sécurité nationale du Canada.

Summary

Accountability in and for National Security

Reg Whitaker and Stuart Farson

In this study, Reg Whitaker and Stuart Farson examine the complex system of accountability that applies to government departments and agencies responsible for Canada's national security and recommend reforms to the system.

Greater accountability in government today is widely supported but imperfectly understood. The concept of accountability must be carefully analyzed, and its objectives clearly specified. Too often, seeking accountability has had unanticipated and even perverse results. National security presents special challenges in this quest, particularly with regard to the extraordinary requirements for secrecy and the complex relationship between intelligence collection and law enforcement.

In examining the issue of accountability in national security, the authors focus on a number of conceptual difficulties, such as the idea of "review" versus that of "oversight." Review – often seen as occurring *ex post facto* – has generally been the preferred option for enhancing accountability in Canada. Whitaker and Farson question whether this focus is appropriate in national security. They find that accountability has mainly been sought for propriety and efficacy, different but interrelated criteria. While review seems most appropriate when dealing with matters of propriety, oversight seems more appropriate when it is a question of efficacy. Thus the authors insist upon widening the scope of how accountability should be understood, to include both review and oversight. They also suggest that an important distinction should be made between accountability *in* (that is, within the executive branch, largely for control purposes) and accountability *for* (that is, the process of accounting by responsible ministers for government actions in and to Parliament) national security.

The study provides an historical overview of how, when and why national security accountability mechanisms developed in Canada. Most often driven by public scandal, accountability reforms have tended to focus on matters of propriety. In the post-9/11 era, there are new challenges from new types of security threats. With new approaches to security, accountability must be adapted to the new realities, involving both propriety and efficacy. The authors conclude that achieving accountability is an evolving but unfinished process.

In the debate over how best to scrutinize Canada's security and intelligence community, the question of what the various bodies and processes are meant to accomplish has not been fully considered. The key question is what powers are available and how they are to be exercised. Three dimensions are of crucial importance: effective access to documents and people; the power to require full and accurate responses; and the process, timing, substance and independence of the reporting procedure.

Whitaker and Farson's recommendations include two central points. First, because national security operations within government and between governments are becoming increasingly integrated, accountability mechanisms should be integrated across institutional boundaries. Second, the role of Parliament in the accountability process needs to be enhanced, in close coordination with existing and enhanced review and oversight bodies. An important caveat is that increased accountability should not hinder the operations of those engaged in protecting Canada's national security.